



# FortiOS - Log Reference

Version 6.4.14

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



June 26, 2023

FortiOS 6.4.14 Log Reference

01-6414-619093-20230626

# TABLE OF CONTENTS

<b>Change Log</b>	<b>29</b>
<b>Introduction</b>	<b>30</b>
Before you begin	30
What's new	31
FortiOS 6.4.14	31
FortiOS 6.4.13	31
FortiOS 6.4.12	31
FortiOS 6.4.11	31
FortiOS 6.4.10	31
FortiOS 6.4.9	32
FortiOS 6.4.8	32
FortiOS 6.4.7	33
FortiOS 6.4.6	33
FortiOS 6.4.5	33
FortiOS 6.4.4	34
FortiOS 6.4.3	34
FortiOS 6.4.2	35
FortiOS 6.4.1	38
FortiOS 6.4.0	39
<b>Log Types and Subtypes</b>	<b>46</b>
Type	46
Subtype	46
List of log types and subtypes	46
UTM log subtypes	47
FortiOS priority levels	49
Log field format	49
<b>Log Schema Structure</b>	<b>50</b>
Log message fields	50
Log ID numbers	53
Log ID definitions	54
<b>FortiGuard Web Filter Categories</b>	<b>57</b>
<b>CEF Support</b>	<b>60</b>
FortiOS to CEF log field mapping guidelines	60
CEF priority levels	60
Examples of CEF support	61
Traffic log support for CEF	61
Event log support for CEF	63
Antivirus log support for CEF	64
Webfilter log support for CEF	65
IPS log support for CEF	66
Email Spamfilter log support for CEF	66
Anomaly log support for CEF	67
VoIP log support for CEF	67

DLP log support for CEF .....	68
Application log support for CEF .....	69
WAF log support for CEF .....	69
DNS log support for CEF .....	69
SSH log support for CEF .....	70
<b>UTM Extended Logging .....</b>	<b>71</b>
Enabling extended logging .....	71
Extended logging option in UTM profiles .....	71
Syslog server mode .....	72
Example of an extended log .....	72
<b>Log Messages .....</b>	<b>73</b>
Anomaly .....	73
18432 - LOGID_ATTCK_ANOMALY_TCP_UDP .....	73
18433 - LOGID_ATTCK_ANOMALY_ICMP .....	74
18434 - LOGID_ATTCK_ANOMALY_OTHERS .....	76
App .....	78
28672 - LOGID_APP_CTRL_IM_BASIC .....	78
28673 - LOGID_APP_CTRL_IM_BASIC_WITH_STATUS .....	80
28674 - LOGID_APP_CTRL_IM_BASIC_WITH_COUNT .....	81
28675 - LOGID_APP_CTRL_IM_FILE .....	83
28676 - LOGID_APP_CTRL_IM_CHAT .....	84
28677 - LOGID_APP_CTRL_IM_CHAT_BLOCK .....	86
28678 - LOGID_APP_CTRL_IM_BLOCK .....	88
28704 - LOGID_APP_CTRL_IPS_PASS .....	89
28705 - LOGID_APP_CTRL_IPS_BLOCK .....	92
28706 - LOGID_APP_CTRL_IPS_RESET .....	94
28720 - LOGID_APP_CTRL_SSH_PASS .....	96
28721 - LOGID_APP_CTRL_SSH_BLOCK .....	98
28736 - LOGID_APP_CTRL_PORT_ENF .....	100
28737 - LOGID_APP_CTRL_PROTO_ENF .....	102
AV .....	105
8192 - MSGID_INFECT_WARNING .....	105
8193 - MSGID_INFECT_NOTIF .....	107
8194 - MSGID_INFECT_MIME_WARNING .....	110
8195 - MSGID_INFECT_MIME_NOTIF .....	112
8200 - MSGID_MIME_FILETYPE_EXE_WARNING .....	115
8201 - MSGID_MIME_FILETYPE_EXE_NOTIF .....	117
8202 - MSGID_AVQUERY_WARNING .....	119
8203 - MSGID_AVQUERY_NOTIF .....	122
8204 - MSGID_MIME_AVQUERY_WARNING .....	124
8205 - MSGID_MIME_AVQUERY_NOTIF .....	127
8212 - MSGID_MALWARE_LIST_WARNING .....	129
8213 - MSGID_MALWARE_LIST_NOTIF .....	132
8214 - MSGID_MIME_MALWARE_LIST_WARNING .....	135
8215 - MSGID_MIME_MALWARE_LIST_NOTIF .....	137
8448 - MSGID_BLOCK_WARNING .....	140
8450 - MSGID_BLOCK_MIME_WARNING .....	142
8451 - MSGID_BLOCK_MIME_NOTIF .....	144

8452 - MESSAGES_BLOCK_COMMAND .....	146
8704 - MESSAGES_OVERSIZE_WARNING .....	148
8705 - MESSAGES_OVERSIZE_NOTIF .....	150
8706 - MESSAGES_OVERSIZE_MIME_WARNING .....	152
8707 - MESSAGES_OVERSIZE_MIME_NOTIF .....	154
8708 - MESSAGES_OVERSIZE_STREAM_UNCOMP_WARNING .....	156
8709 - MESSAGES_OVERSIZE_STREAM_UNCOMP_NOTIF .....	158
8720 - MESSAGES_SWITCH_PROTO_WARNING .....	160
8721 - MESSAGES_SWITCH_PROTO_NOTIF .....	162
8960 - MESSAGES_SCAN_UNCOMPSIZELIMIT_WARNING .....	163
8961 - MESSAGES_SCAN_UNCOMPSIZELIMIT_NOTIF .....	166
8962 - MESSAGES_SCAN_ARCHIVE_ENCRYPTED_WARNING .....	168
8963 - MESSAGES_SCAN_ARCHIVE_ENCRYPTED_NOTIF .....	171
8964 - MESSAGES_SCAN_ARCHIVE_CORRUPTED_WARNING .....	173
8965 - MESSAGES_SCAN_ARCHIVE_CORRUPTED_NOTIF .....	176
8966 - MESSAGES_SCAN_ARCHIVE_MULTIPART_WARNING .....	179
8967 - MESSAGES_SCAN_ARCHIVE_MULTIPART_NOTIF .....	181
8968 - MESSAGES_SCAN_ARCHIVE_NESTED_WARNING .....	184
8969 - MESSAGES_SCAN_ARCHIVE_NESTED_NOTIF .....	186
8970 - MESSAGES_SCAN_ARCHIVE_OVERSIZE_WARNING .....	189
8971 - MESSAGES_SCAN_ARCHIVE_OVERSIZE_NOTIF .....	191
8972 - MESSAGES_SCAN_ARCHIVE_UNHANDLED_WARNING .....	194
8973 - MESSAGES_SCAN_ARCHIVE_UNHANDLED_NOTIF .....	196
8974 - MESSAGES_SCAN_AV_ENGINE_LOAD_FAILED_ERROR .....	199
8975 - MESSAGES_SCAN_ARCHIVE_PARTIALLYCORRUPTED_WARNING .....	202
8976 - MESSAGES_SCAN_ARCHIVE_PARTIALLYCORRUPTED_NOTIF .....	204
8977 - MESSAGES_SCAN_ARCHIVE_FILESLIMIT_WARNING .....	207
8978 - MESSAGES_SCAN_ARCHIVE_FILESLIMIT_NOTIF .....	209
8979 - MESSAGES_SCAN_ARCHIVE_TIMEOUT_WARNING .....	212
8980 - MESSAGES_SCAN_ARCHIVE_TIMEOUT_NOTIF .....	214
8981 - MESSAGES_SCAN_AV_CDR_INTERNAL_ERROR .....	217
9233 - MESSAGES_ANALYTICS_SUBMITTED .....	219
9234 - MESSAGES_ANALYTICS_INFECT_WARNING .....	222
9235 - MESSAGES_ANALYTICS_INFECT_NOTIF .....	225
9236 - MESSAGES_ANALYTICS_INFECT_MIME_WARNING .....	227
9237 - MESSAGES_ANALYTICS_INFECT_MIME_NOTIF .....	230
9238 - MESSAGES_ANALYTICS_FSA_RESULT .....	232
9239 - MESSAGES_CONTENT_DISARM_NOTIF .....	233
9240 - MESSAGES_CONTENT_DISARM_WARNING .....	236
CIFS .....	238
63000 - LOG_ID_CIFS_FILE_BLOCK .....	238
63001 - LOG_ID_CIFS_FILE_PASS .....	239
63002 - LOG_ID_CIFS_CONN_FAIL .....	241
63003 - LOG_ID_CIFS_AUTH_FAIL .....	242
63004 - LOG_ID_CIFS_AUTH_INTERNAL_ERROR .....	244
63005 - LOG_ID_CIFS_AUTH_KRB_ERROR .....	245
DLP .....	247
24576 - LOG_ID_DLP_WARN .....	247
24577 - LOG_ID_DLP_NOTIF .....	249

DNS .....	252
54000 - LOG_ID_DNS_QUERY .....	252
54200 - LOG_ID_DNS_RESOLV_ERROR .....	253
54400 - LOG_ID_DNS_URL_FILTER_BLOCK .....	255
54401 - LOG_ID_DNS_URL_FILTER_ALLOW .....	257
54600 - LOG_ID_DNS_BOTNET_IP .....	259
54601 - LOG_ID_DNS_BOTNET_DOMAIN .....	261
54800 - LOG_ID_DNS_FTGD_WARNING .....	263
54801 - LOG_ID_DNS_FTGD_ERROR .....	265
54802 - LOG_ID_DNS_FTGD_CAT_ALLOW .....	267
54803 - LOG_ID_DNS_FTGD_CAT_BLOCK .....	269
54804 - LOG_ID_DNS_SAFE_SEARCH .....	271
Email .....	273
20480 - LOGID_ANTISPAM_EMAIL_NOTIF .....	273
20481 - LOGID_EMAIL_GENERAL_NOTIF .....	275
20482 - LOGID_ANTISPAM_EMAIL_BWORD_NOTIF .....	277
20509 - LOGID_ANTISPAM_FTGD_ERR .....	278
20510 - LOGID_ANTISPAM_EMAIL_WEBMAIL_NOTIF .....	280
Event .....	282
20002 - LOG_ID_DOMAIN_UNRESOLVABLE .....	282
20003 - LOG_ID_MAIL_SENT_FAIL .....	283
20004 - LOG_ID_POLICY_TOO_BIG .....	284
20005 - LOG_ID_PPP_LINK_UP .....	285
20006 - LOG_ID_PPP_LINK_DOWN .....	285
20007 - LOG_ID_SOCKET_EXHAUSTED .....	286
20008 - LOG_ID_POLICY6_TOO_BIG .....	287
20010 - LOG_ID_KERNEL_ERROR .....	288
20016 - LOG_ID_MODEM_EXCEED_REDIAL_COUNT .....	289
20017 - LOG_ID_MODEM_FAIL_TO_OPEN .....	289
20020 - LOG_ID_MODEM_USB_DETECTED .....	290
20021 - LOG_ID_MAIL_RESENT .....	291
20022 - LOG_ID_MODEM_USB_REMOVED .....	291
20023 - LOG_ID_MODEM_USBLTE_DETECTED .....	292
20024 - LOG_ID_MODEM_USBLTE_REMOVED .....	293
20025 - LOG_ID_REPORTD_REPORT_SUCCESS .....	293
20026 - LOG_ID_REPORTD_REPORT_FAILURE .....	294
20028 - LOG_ID_REPORT_RECREATE_DB .....	295
20031 - LOG_ID_RAD_OUT_OF_MEM .....	296
20032 - LOG_ID_RAD_NOT_FOUND .....	296
20033 - LOG_ID_RAD_MOBILE_IPV6 .....	297
20034 - LOG_ID_RAD_IPV6_OUT_OF_RANGE .....	298
20035 - LOG_ID_RAD_MIN_OUT_OF_RANGE .....	298
20036 - LOG_ID_RAD_MAX_OUT_OF_RANGE .....	299
20037 - LOG_ID_RAD_MAX_ADV_OUT_OF_RANGE .....	300
20039 - LOG_ID_RAD_MTU_TOO_SMALL .....	300
20040 - LOG_ID_RAD_TIME_TOO_SMALL .....	301
20041 - LOG_ID_RAD_HOP_OUT_OF_RANGE .....	302
20042 - LOG_ID_RAD_DFT_HOP_OUT_OF_RANGE .....	302
20043 - LOG_ID_RAD_AGENT_OUT_OF_RANGE .....	303

20044 - LOG_ID_RAD_AGENT_FLAG_NOT_SET .....	304
20045 - LOG_ID_RAD_PREFIX_TOO_LONG .....	304
20046 - LOG_ID_RAD_PREF_TIME_TOO_SMALL .....	305
20047 - LOG_ID_RAD_FAIL_IPV6_SOCKET .....	306
20048 - LOG_ID_RAD_FAIL_OPT_IPV6_PKTINFO .....	306
20049 - LOG_ID_RAD_FAIL_OPT_IPV6_CHECKSUM .....	307
20050 - LOG_ID_RAD_FAIL_OPT_IPV6_UNICAST_HOPS .....	308
20051 - LOG_ID_RAD_FAIL_OPT_IPV6_MULTICAST_HOPS .....	308
20052 - LOG_ID_RAD_FAIL_OPT_IPV6_HOPLIMIT .....	309
20053 - LOG_ID_RAD_FAIL_OPT_IPPROTO_ICMPV6 .....	310
20054 - LOG_ID_RAD_EXIT_BY_SIGNAL .....	310
20055 - LOG_ID_RAD_FAIL_CMDB_QUERY .....	311
20056 - LOG_ID_RAD_FAIL_CMDB_FOR_EACH .....	312
20057 - LOG_ID_RAD_FAIL_FIND_VIRT_INTF .....	312
20058 - LOG_ID_RAD_UNLOAD_INTF .....	313
20061 - LOG_ID_RAD_INV_ICMPV6_TYPE .....	314
20062 - LOG_ID_RAD_INV_ICMPV6_RA_LEN .....	314
20063 - LOG_ID_RAD_ICMPV6_NO_SRC_ADDR .....	315
20064 - LOG_ID_RAD_INV_ICMPV6_RS_LEN .....	316
20065 - LOG_ID_RAD_INV_ICMPV6_CODE .....	316
20066 - LOG_ID_RAD_INV_ICMPV6_HOP .....	317
20067 - LOG_ID_RAD_MISMATCH_HOP .....	318
20068 - LOG_ID_RAD_MISMATCH_MGR_FLAG .....	318
20069 - LOG_ID_RAD_MISMATCH_OTH_FLAG .....	319
20070 - LOG_ID_RAD_MISMATCH_TIME .....	320
20071 - LOG_ID_RAD_MISMATCH_TIMER .....	320
20072 - LOG_ID_RAD_EXTRA_DATA .....	321
20073 - LOG_ID_RAD_NO_OPT_DATA .....	322
20074 - LOG_ID_RAD_INV_OPT_LEN .....	322
20075 - LOG_ID_RAD_MISMATCH_MTU .....	323
20077 - LOG_ID_RAD_MISMATCH_PREF_TIME .....	324
20078 - LOG_ID_RAD_INV_OPT .....	324
20080 - LOG_ID_RAD_FAIL_TO_RCV .....	325
20081 - LOG_ID_RAD_INV_HOP .....	326
20082 - LOG_ID_RAD_INV_PKTINFO .....	326
20083 - LOG_ID_RAD_FAIL_TO_CHECK .....	327
20084 - LOG_ID_RAD_FAIL_TO_SEND .....	328
20085 - LOG_ID_SESSION_CLASH .....	328
20090 - LOG_ID_INTF_LINK_STA_CHG .....	329
20099 - LOG_ID_INTF_STA_CHG .....	330
20100 - LOG_ID_WEB_CAT_UPDATED .....	331
20101 - LOG_ID_WEB_LIC_EXPIRE .....	331
20102 - LOG_ID_SPAM_LIC_EXPIRE .....	332
20103 - LOG_ID_AV_LIC_EXPIRE .....	333
20104 - LOG_ID_IPS_LIC_EXPIRE .....	333
20107 - LOG_ID_LOG_UPLOAD_ERR .....	334
20108 - LOG_ID_LOG_UPLOAD_DONE .....	335
20109 - LOG_ID_WEB_LIC_EXPIRED .....	336
20113 - LOG_ID_IPSA_DOWNLOAD_FAIL .....	336

20114 - LOG_ID_IPSA_SELFTEST_FAIL .....	337
20115 - LOG_ID_IPSA_STATUSUPD_FAIL .....	338
20116 - LOG_ID_SPAM_LIC_EXPIRED .....	338
20117 - LOG_ID_AV_LIC_EXPIRED .....	339
20118 - LOG_ID_WEBF_STATUS_REACH .....	340
20119 - LOG_ID_WEBF_STATUS_UNREACH .....	340
20200 - LOG_ID_FIPS_SELF_TEST .....	341
20201 - LOG_ID_FIPS_SELF_ALL_TEST .....	342
20202 - LOG_ID_DISK_FORMAT_ERROR .....	343
20203 - LOG_ID_DAEMON_SHUTDOWN .....	343
20204 - LOG_ID_DAEMON_START .....	344
20205 - LOG_ID_DISK_FORMAT_REQ .....	345
20206 - LOG_ID_DISK_SCAN_REQ .....	346
20207 - LOG_ID_RAD_MISMATCH_VALID_TIME .....	346
20208 - LOG_ID_ZOMBIE_DAEMON_CLEANUP .....	347
20209 - LOG_ID_DISK_UNAVAIL .....	348
20210 - LOG_ID_DISK_TRIM_START .....	348
20211 - LOG_ID_DISK_TRIM_END .....	349
20212 - LOG_ID_DISK_SCAN_NEEDED .....	350
20213 - LOG_ID_DISK_LOG_CORRUPTED .....	351
20220 - LOGID_EVENT_SHAPER_OUTBOUND_MAXED_OUT .....	351
20221 - LOGID_EVENT_SHAPER_INBOUND_MAXED_OUT .....	352
20230 - LOG_ID_SYS_SECURITY_WRITE_VIOLATION .....	353
20231 - LOG_ID_SYS_SECURITY_HARDLINK_VIOLATION .....	353
20232 - LOG_ID_SYS_SECURITY_LOAD_MODULE_VIOLATION .....	354
20233 - LOG_ID_SYS_SECURITY_FILE_HASH_MISSING .....	355
20234 - LOG_ID_SYS_SECURITY_FILE_HASH_MISMATCH .....	355
20300 - LOG_ID_BGP_NB_STAT_CHG .....	356
20301 - LOG_ID_VZ_LOG .....	357
20302 - LOG_ID_OSPF_NB_STAT_CHG .....	357
20303 - LOG_ID_OSPF6_NB_STAT_CHG .....	358
20401 - LOG_ID_ROUTER_CLEAR .....	359
22000 - LOG_ID_INV_PKT_LEN .....	360
22001 - LOG_ID_UNSUPPORTED_PROT_VER .....	360
22002 - LOG_ID_INV_REQ_TYPE .....	361
22003 - LOG_ID_FAIL_SET_SIG_HANDLER .....	362
22004 - LOG_ID_FAIL_CREATE_SOCKET .....	362
22005 - LOG_ID_FAIL_CREATE_SOCKET_RETRY .....	363
22006 - LOG_ID_FAIL_REG_CMDB_EVENT .....	364
22009 - LOG_ID_FAIL_FIND_AV_PROFILE .....	364
22010 - LOG_ID_SENDTO_FAIL .....	365
22011 - LOG_ID_ENTER_MEM_CONSERVE_MODE .....	366
22012 - LOG_ID_LEAVE_MEM_CONSERVE_MODE .....	367
22013 - LOG_ID_IPPOOLPBA_BLOCK_EXHAUSTED .....	368
22014 - LOG_ID_IPPOOLPBA_NATIP_EXHAUSTED .....	368
22015 - LOG_ID_IPPOOLPBA_CREATE .....	369
22016 - LOG_ID_IPPOOLPBA_DEALLOCATE .....	370
22017 - LOG_ID_EXCEED_GLOB_RES_LIMIT .....	371
22018 - LOG_ID_EXCEED_VD_RES_LIMIT .....	372



22019 - LOG_ID_LOGRATE_OVER_LIMIT .....	372
22020 - LOG_ID_FAIL_CREATE_HA_SOCKET .....	373
22021 - LOG_ID_FAIL_CREATE_HA_SOCKET_RETRY .....	374
22031 - LOG_ID_SUCCESS_CSF_LOG_SYNC_CONFIG_CHANGED .....	374
22032 - LOG_ID_CSF_LOOP_FOUND .....	375
22035 - LOG_ID_CSF_UPSTREAM_SN_CHANGED .....	376
22036 - LOG_ID_CSF_FGT_CONNECTED .....	377
22037 - LOG_ID_CSF_FGT_DISCONNECTED .....	378
22038 - LOG_ID_CSF_GLOBAL_SYNC_FAILED .....	378
22039 - LOG_ID_CSF_GLOBAL_SYNC_REPORT .....	379
22050 - LOG_ID_IPAMD_ADDRESS_ALLOCATED .....	380
22051 - LOG_ID_IPAMD_ADDRESS_SET_FAILED .....	381
22052 - LOG_ID_IPAMD_ADDRESS_INVALIDATED .....	382
22053 - LOG_ID_IPAMD_VALIDATION_COMPLETE .....	382
22100 - LOG_ID_QUAR_DROP_TRAN_JOB .....	383
22101 - LOG_ID_QUAR_DROP_TLL_JOB .....	384
22102 - LOG_ID_LOG_DISK_FAILURE .....	385
22103 - LOG_ID_QUAR_LIMIT_REACHED .....	385
22104 - LOG_ID_POWER_RESTORE .....	386
22105 - LOG_ID_POWER_FAILURE .....	387
22106 - LOG_ID_POWER_OPTIONAL_NOT_DETECTED .....	388
22107 - LOG_ID_VOLT_ANOM .....	389
22108 - LOG_ID_FAN_ANOM .....	389
22109 - LOG_ID_TEMP_TOO_HIGH .....	390
22110 - LOG_ID_SPARE_BLOCK_LOW .....	391
22113 - LOG_ID_FNBAM_FAILURE .....	391
22114 - LOG_ID_POWER_REDUNDANCY_DEGRADE .....	392
22115 - LOG_ID_POWER_REDUNDANCY_FAILURE .....	393
22150 - LOG_ID_VOLT_NOM .....	394
22151 - LOG_ID_FAN_NOM .....	394
22152 - LOG_ID_TEMP_TOO_LOW .....	395
22153 - LOG_ID_TEMP_NORM .....	396
22200 - LOG_ID_AUTO_UPT_CERT .....	397
22201 - LOG_ID_AUTO_GEN_CERT .....	398
22203 - LOG_ID_AUTO_GEN_CERT_FAIL .....	398
22204 - LOG_ID_AUTO_GEN_CERT_PENDING .....	399
22205 - LOG_ID_AUTO_GEN_CERT_SUCC .....	400
22206 - LOG_ID_CRL_EXPIRED .....	401
22220 - LOG_ID_EXT_RESOURCE .....	402
22221 - LOG_ID_EXT_RESOURCE_FAIL .....	402
22222 - LOG_ID_EXT_RESOURCE_LOAD .....	403
22223 - LOG_ID_EXT_RESOURCE_DEBUG .....	404
22700 - LOG_ID_IPS_FAIL_OPEN .....	405
22701 - LOG_ID_IPS_FAIL_OPEN_END .....	406
22800 - LOG_ID_SCAN_SERV_FAIL .....	406
22802 - LOG_ID_ENTER_FD_CONSERVE_MODE .....	407
22803 - LOG_ID_LEAVE_FD_CONSERVE_MODE .....	408
22804 - LOG_ID_LIC_STATUS_CHG .....	409
22805 - LOG_ID_FAIL_TO_VALIDATE_LIC .....	410

22806 - LOG_ID_DUP_LIC .....	411
22807 - LOG_ID_VDOM_LIC .....	411
22808 - LOG_ID_LIC_EXPIRE .....	412
22809 - LOG_ID_LIC_WILL_EXPIRE .....	413
22810 - LOG_ID_SCANUNIT_ERROR_BLOCK .....	414
22811 - LOG_ID_SCANUNIT_ERROR_PASS .....	415
22812 - LOG_ID_SCANUNIT_AVENG_RELOAD .....	416
22813 - LOG_ID_SCANUNIT_AVDB_RELOAD .....	417
22814 - LOG_ID_SCANUNIT_AVDB_RELOAD_ERROR .....	417
22815 - LOG_ID_SCANUNIT_AVDB_LOAD .....	418
22816 - LOG_ID_SCANUNIT_AVDB_LOAD_ERROR .....	419
22850 - LOG_ID_USER_QUARANTINE_MAC_ADD .....	419
22851 - LOG_ID_USER_QUARANTINE_MAC_DELETE .....	420
22852 - LOG_ID_USER_QUARANTINE_MAC_BOUNCE_PORT_HIT .....	421
22853 - LOG_ID_USER_QUARANTINE_MAC_BOUNCE_PORT_MISS .....	422
22890 - LOG_ID_FORTILINKD .....	423
22891 - LOG_ID_FLCFGD_SYNC_ERROR .....	424
22892 - LOG_ID_FLCFGD_SYNC_COMPLETE .....	424
22893 - LOG_ID_FLCFGD_SYNC_STATE .....	425
22894 - LOG_ID_FLCFGD_UPGRADE_ERROR .....	426
22895 - LOG_ID_FLCFGD_UPGRADE_STATUS .....	427
22896 - LOG_ID_FORTILINKD_CRITICAL .....	428
22897 - LOG_ID_FLCFGD_NAC_ADD .....	428
22898 - LOG_ID_FLCFGD_NAC_DELETE .....	429
22899 - LOG_ID_FLCFGD_NAC_MODIFY .....	430
22900 - LOG_ID_CAPUTP_SESSION .....	431
22901 - LOG_ID_FAZ_CON .....	432
22902 - LOG_ID_FAZ_DISCON .....	432
22903 - LOG_ID_FAZ_CON_ERR .....	433
22904 - LOG_ID_CAPUTP_SESSION_NOTIF .....	434
22912 - LOG_ID_FDS_SRV_ERRCON .....	435
22913 - LOG_ID_FDS_SRV_DISCON .....	436
22914 - LOG_ID_FDS_SRV_CHG .....	436
22915 - LOG_ID_FDS_SRV_CON .....	437
22916 - LOG_ID_FDS_STATUS .....	438
22917 - LOG_ID_FDS_SMS_QUOTA .....	439
22918 - LOG_ID_FDS_CTRL_STATUS .....	439
22919 - LOG_ID_SVR_LOG_STATUS_CHANGED .....	440
22921 - LOG_ID_EVENT_ROUTE_INFO_CHANGED .....	441
22922 - LOG_ID_EVENT_LINK_MONITOR_STATUS .....	441
22923 - LOG_ID_EVENT_VWL_LQTY_STATUS .....	442
22924 - LOG_ID_EVENT_VWL_VOLUME_STATUS .....	443
22925 - LOG_ID_EVENT_VWL_SLA_INFO .....	444
22926 - LOG_ID_EVENT_VWL_NEIGHBOR_STATUS .....	445
22927 - LOG_ID_EVENT_VWL_NEIGHBOR_STANDALONE .....	446
22928 - LOG_ID_EVENT_VWL_NEIGHBOR_PRIMARY .....	447
22929 - LOG_ID_EVENT_VWL_NEIGHBOR_SECONDARY .....	448
22949 - LOG_ID_FDS_JOIN .....	448
22950 - LOG_ID_FDS_LOGIN_SUCC .....	449

22951 - LOG_ID_FDS_LOGOUT .....	450
22952 - LOG_ID_FDS_LOGIN_FAIL .....	451
22953 - LOG_ID_IOC_DETECTED .....	451
22954 - LOG_ID_INET_SVC_OBSOLETE .....	452
22955 - LOG_ID_INET_SVC_NAME_FAILURE .....	453
22956 - LOG_ID_INET_SVC_NAME_UPDATE .....	453
23101 - LOG_ID_IPSEC_TUNNEL_UP .....	454
23102 - LOG_ID_IPSEC_TUNNEL_DOWN .....	455
23103 - LOG_ID_IPSEC_TUNNEL_STAT .....	456
26001 - LOG_ID_DHCP_ACK .....	457
26002 - LOG_ID_DHCP_RELEASE .....	458
26003 - LOG_ID_DHCP_STAT .....	459
26004 - LOG_ID_DHCP_CLIENT_LEASE .....	459
26005 - LOG_ID_DHCP_LEASE_USAGE_HIGH .....	460
26006 - LOG_ID_DHCP_LEASE_USAGE_FULL .....	461
26007 - LOG_ID_DHCP_BLOCKED_MAC .....	462
26008 - LOG_ID_DHCP_DDNS_ADD .....	462
26009 - LOG_ID_DHCP_DDNS_DELETE .....	463
26010 - LOG_ID_DHCP_DDNS_COMPLETED .....	464
26011 - LOG_ID_DHCPV6_REPLY .....	465
26012 - LOG_ID_DHCPV6_RELEASE .....	466
27001 - LOG_ID_VRRP_STATE_CHG .....	467
29001 - LOG_ID_PPPD_MSG .....	467
29002 - LOG_ID_PPPD_AUTH_SUC .....	468
29003 - LOG_ID_PPPD_AUTH_FAIL .....	469
29010 - LOG_ID_PPPOE_STATUS_REPORT_NOTIF .....	470
29011 - LOG_ID_PPPD_FAIL_TO_EXEC .....	471
29012 - LOG_ID_PPP_OPT_ERR .....	471
29013 - LOG_ID_PPPD_START .....	472
29014 - LOG_ID_PPPD_EXIT .....	473
29015 - LOG_ID_PPP_RCV_BAD_PEER_IP .....	473
29016 - LOG_ID_PPP_RCV_BAD_LOCAL_IP .....	474
29017 - LOG_ID_PPP_OPT_NOTIF .....	475
29021 - LOG_ID_EVENT_AUTH_SNMP_QUERY_FAILED .....	475
29022 - LOG_ID_DDNS_UPDATE_FAIL .....	476
32001 - LOG_ID_ADMIN_LOGIN_SUCC .....	477
32002 - LOG_ID_ADMIN_LOGIN_FAIL .....	478
32003 - LOG_ID_ADMIN_LOGOUT .....	479
32005 - LOG_ID_ADMIN_OVERRIDE_VDOM .....	480
32006 - LOG_ID_ADMIN_ENTER_VDOM .....	481
32007 - LOG_ID_ADMIN_LEFT_VDOM .....	482
32008 - LOG_ID_VIEW_DISK_LOG_FAIL .....	482
32009 - LOG_ID_SYSTEM_START .....	483
32010 - LOG_ID_DISK_LOG_FULL .....	484
32011 - LOG_ID_LOG_ROLL .....	485
32014 - LOG_ID_CS_LIC_EXPIRE .....	485
32015 - LOG_ID_DISK_LOG_USAGE .....	486
32017 - LOG_ID_FDS_DAILY_QUOTA_FULL .....	487
32018 - LOG_ID_FIPS_ENTER_ERR_MOD .....	487

32019 - LOG_ID_CC_ENTER_ERR_MOD .....	488
32020 - LOG_ID_SSH_CORRPUT_MAC .....	489
32021 - LOG_ID_ADMIN_LOGIN_DISABLE .....	490
32022 - LOG_ID_VDOM_ENABLED .....	490
32023 - LOG_ID_MEM_LOG_FIRST_FULL .....	491
32024 - LOG_ID_ADMIN_PASSWD_EXPIRE .....	492
32025 - LOG_ID_SSH_REKEY .....	493
32026 - LOG_ID_SSH_BAD_PACKET_LENGTH .....	493
32027 - LOG_ID_VIEW_DISK_LOG_SUCC .....	494
32028 - LOG_ID_LOG_DEL_DIR .....	495
32029 - LOG_ID_LOG_DEL_FILE .....	495
32030 - LOG_ID_SEND_FDS_STAT .....	496
32031 - LOG_ID_VIEW_MEM_LOG_FAIL .....	497
32032 - LOG_ID_DISK_DLP_ARCH_FULL .....	498
32033 - LOG_ID_DISK_QUAR_FULL .....	498
32034 - LOG_ID_DISK_REPORT_FULL .....	499
32035 - LOG_ID_VDOM_DISABLED .....	500
32036 - LOG_ID_DISK_IPS_ARCH_FULL .....	500
32037 - LOG_ID_DISK_LOG_FIRST_FULL .....	501
32038 - LOG_ID_LOG_ROLL_FORTICRON .....	502
32039 - LOG_ID_VIEW_MEM_LOG_SUCC .....	503
32040 - LOG_ID_REPORT_DELETED .....	503
32041 - LOG_ID_REPORT_DELETED_GUI .....	504
32042 - LOG_ID_MEM_LOG_SECOND_FULL .....	505
32043 - LOG_ID_MEM_LOG_FINAL_FULL .....	505
32044 - LOG_ID_LOG_DELETE .....	506
32045 - LOG_ID_MGR_LIC_EXPIRE .....	507
32048 - LOG_ID_SCHEDULE_EXPIRE .....	508
32049 - LOG_ID_FC_EXPIRE .....	508
32050 - LOG_ID_POL_PKT_CAPTURE_FULL .....	509
32051 - LOG_ID_LOG_UPLOAD .....	510
32052 - LOG_ID_UPLOAD_RUN_SCRIPT .....	510
32053 - LOG_ID_ADMIN_MTNER_LOGIN_SUCC .....	511
32054 - LOG_ID_ADMIN_MTNER_LOGOUT .....	512
32057 - LOG_ID_VIEW_FAZ_LOG_FAIL .....	513
32058 - LOG_ID_VIEW_FAZ_LOG_SUCC .....	514
32095 - LOG_ID_GUI_CHG_SUB_MODULE .....	515
32096 - LOG_ID_GUI_DOWNLOAD_LOG .....	515
32097 - LOG_ID_DELETE_CAPTURE_PKT .....	516
32100 - LOG_ID_FORTI_TOKEN_SYNC .....	517
32102 - LOG_ID_CHG_CONFIG .....	518
32103 - LOG_ID_NEW_FIRMWARE .....	519
32104 - LOG_ID_CHG_CONFIG_GUI .....	519
32105 - LOG_ID_NTP_SVR_STAUS_CHG_REACHABLE .....	520
32106 - LOG_ID_NTP_SVR_STAUS_CHG_RESOLVABLE .....	521
32107 - LOG_ID_NTP_SVR_STAUS_CHG_UNRESOLVABLE .....	522
32108 - LOG_ID_NTP_SVR_STAUS_CHG_UNREACHABLE .....	523
32109 - LOG_ID_UPD_SIGN_AV_DB .....	523
32110 - LOG_ID_UPD_SIGN_IPS_DB .....	524

32111 - LOG_ID_UPD_SIGN_AVIPS_DB .....	525
32113 - LOG_ID_UPD_SIGN_SRCVIS_DB .....	526
32114 - LOG_ID_UPD_SIGN_GEOIP_DB .....	527
32116 - LOG_ID_UPD_SIGN_AVPKG_FAILURE .....	527
32117 - LOG_ID_UPD_SIGN_AVPKG_SUCCESS .....	528
32118 - LOG_ID_UPD_ADMIN_AV_DB .....	529
32119 - LOG_ID_UPD_SCANUNIT_AV_DB .....	530
32120 - LOG_ID_RPT_ADD_DATASET .....	530
32122 - LOG_ID_RPT_DEL_DATASET .....	531
32125 - LOG_ID_RPT_ADD_CHART .....	532
32126 - LOG_ID_RPT_DEL_CHART .....	533
32129 - LOG_ID_ADD_GUEST .....	533
32130 - LOG_ID_CHG_USER .....	534
32131 - LOG_ID_DEL_GUEST .....	535
32132 - LOG_ID_ADD_USER .....	536
32138 - LOG_ID_REBOOT .....	537
32139 - LOG_ID_WAKE_ON_LAN .....	538
32140 - LOG_ID_TIME_USER_SETTING_CHG .....	538
32141 - LOG_ID_TIME_NTP_SETTING_CHG .....	539
32142 - LOG_ID_BACKUP_CONF .....	540
32143 - LOG_ID_BACKUP_CONF_BY_SCP .....	541
32144 - LOG_ID_BACKUP_CONF_ERROR .....	542
32145 - LOG_ID_BACKUP_CONF_ALERT .....	542
32146 - LOG_ID_TIME_PTP_SETTING_CHG .....	543
32148 - LOG_ID_GET_CRL .....	544
32149 - LOG_ID_COMMAND_FAIL .....	545
32151 - LOG_ID_ADD_IP6_LOCAL_POL .....	545
32152 - LOG_ID_CHG_IP6_LOCAL_POL .....	546
32153 - LOG_ID_DEL_IP6_LOCAL_POL .....	547
32155 - LOG_ID_ACT_FTOKEN_REQ .....	548
32156 - LOG_ID_ACT_FTOKEN_SUCC .....	548
32157 - LOG_ID_SYNC_FTOKEN_SUCC .....	549
32158 - LOG_ID_SYNC_FTOKEN_FAIL .....	550
32159 - LOG_ID_ACT_FTOKEN_FAIL .....	551
32160 - LOG_ID_FTM_PUSH_SUCC .....	552
32161 - LOG_ID_FTM_PUSH_FAIL .....	552
32168 - LOG_ID_REACH_VDOM_LIMIT .....	553
32169 - LOG_ID_ALARM_DLP_DB .....	554
32170 - LOG_ID_ALARM_MSG .....	555
32171 - LOG_ID_ALARM_ACK .....	555
32172 - LOG_ID_ADD_IP4_LOCAL_POL .....	556
32173 - LOG_ID_CHG_IP4_LOCAL_POL .....	557
32174 - LOG_ID_DEL_IP4_LOCAL_POL .....	558
32190 - LOG_ID_UPT_INVALID_IMG .....	559
32191 - LOG_ID_UPT_INVALID_IMG_CC .....	559
32192 - LOG_ID_UPT_INVALID_IMG_RSA .....	560
32193 - LOG_ID_UPT_IMG_RSA .....	561
32194 - LOG_ID_UPT_IMG_FAIL .....	562
32199 - LOG_ID_RESTORE_IMG_USB .....	562

32200 - LOG_ID_SHUTDOWN .....	563
32201 - LOG_ID_LOAD_IMG_SUCC .....	564
32202 - LOG_ID_RESTORE_IMG .....	565
32203 - LOG_ID_RESTORE_CONF .....	566
32204 - LOG_ID_RESTORE_FGD_SVR .....	566
32205 - LOG_ID_RESTORE_VDOM_LIC .....	567
32206 - LOG_ID_RESTORE_SCRIPT .....	568
32207 - LOG_ID_RETRIEVE_CONF_LIST .....	569
32208 - LOG_ID_IMP_PKCS12_CERT .....	570
32209 - LOG_ID_RESTORE_USR_DEF_IPS .....	570
32210 - LOG_ID_BACKUP_IMG_SUCC .....	571
32211 - LOG_ID_UPLOAD_REVISION .....	572
32212 - LOG_ID_DEL_REVISION .....	573
32213 - LOG_ID_RESTORE_TEMPLATE .....	574
32214 - LOG_ID_RESTORE_FILE .....	574
32215 - LOG_ID_UPT_IMG .....	575
32217 - LOG_ID_UPD_IPS .....	576
32218 - LOG_ID_UPD_DLP .....	577
32219 - LOG_ID_BACKUP_OUTPUT .....	577
32220 - LOG_ID_BACKUP_COMMAND .....	578
32221 - LOG_ID_UPD_VDOM_LIC .....	579
32222 - LOG_ID_GLB_SETTING_CHG .....	580
32223 - LOG_ID_BACKUP_USER_DEF_IPS .....	581
32224 - LOG_ID_BACKUP_DISK_LOG .....	581
32225 - LOG_ID_DEL_ALL_REVISION .....	582
32226 - LOG_ID_LOAD_IMG_FAIL .....	583
32227 - LOG_ID_UPD_DLP_FAIL .....	584
32228 - LOG_ID_LOAD_IMG_FAIL_WRONG_IMG .....	585
32229 - LOG_ID_LOAD_IMG_FAIL_NO_RSA .....	585
32230 - LOG_ID_LOAD_IMG_FAIL_INVALID_RSA .....	586
32231 - LOG_ID_RESTORE_FGD_SVR_FAIL .....	587
32232 - LOG_ID_RESTORE_VDOM_LIC_FAIL .....	588
32233 - LOG_ID_BACKUP_IMG_FAIL .....	588
32234 - LOG_ID_RESTORE_IMG_INVALID_CC .....	589
32235 - LOG_ID_RESTORE_IMG_FORTIGUARD .....	590
32236 - LOG_ID_BACKUP_MEM_LOG .....	591
32237 - LOG_ID_BACKUP_MEM_LOG_FAIL .....	591
32238 - LOG_ID_BACKUP_DISK_LOG_FAIL .....	592
32239 - LOG_ID_BACKUP_DISK_LOG_USB .....	593
32240 - LOG_ID_SYS_USB_MODE .....	594
32241 - LOG_ID_BACKUP_DISK_LOG_USB_FAIL .....	595
32242 - LOG_ID_UPD_VDOM_LIC_FAIL .....	595
32243 - LOG_ID_UPD_IPS_SCP .....	596
32244 - LOG_ID_UPD_IPS_SCP_FAIL .....	597
32245 - LOG_ID_BACKUP_USER_DEF_IPS_FAIL .....	598
32246 - LOG_ID_RESTORE_USR_DEF_IPS_CRITICAL .....	598
32247 - LOG_ID_SSH_NEGOTIATION_FAILURE .....	599
32252 - LOG_ID_FACTORY_RESET .....	600
32253 - LOG_ID_FORMAT_RAID .....	601

32254 - LOG_ID_ENABLE_RAID .....	602
32255 - LOG_ID_DISABLE_RAID .....	602
32262 - LOG_ID_RESTORE_IMG_CONFIRM .....	603
32300 - LOG_ID_UPLOAD_RPT_IMG .....	604
32301 - LOG_ID_ADD_VDOM .....	605
32302 - LOG_ID_DEL_VDOM .....	606
32545 - LOG_ID_SYS_RESTART .....	606
32546 - LOG_ID_APPLICATION_CRASH .....	607
32547 - LOG_ID_AUTOSCRIPT_START .....	608
32548 - LOG_ID_AUTOSCRIPT_STOP .....	609
32549 - LOG_ID_AUTOSCRIPT_STOP_AUTO .....	610
32550 - LOG_ID_AUTOSCRIPT_DELETE_RSLT .....	610
32551 - LOG_ID_AUTOSCRIPT_BACKUP_RSLT .....	611
32552 - LOG_ID_AUTOSCRIPT_CHECK_STATUS .....	612
32553 - LOG_ID_AUTOSCRIPT_STOP_REACH_LIMIT .....	613
32561 - LOG_ID_ADMIN_LOGOUT_DISCONNECT .....	613
32562 - LOG_ID_STORE_CONF_FAIL_SPACE .....	614
32564 - LOG_ID_RESTORE_CONF_FAIL .....	615
32565 - LOG_ID_RESTORE_CONF_BY_MGMT .....	616
32566 - LOG_ID_RESTORE_CONF_BY_SCP .....	617
32567 - LOG_ID_RESTORE_CONF_BY_USB .....	617
32568 - LOG_ID_DEL_REVISION_DB .....	618
32569 - LOG_ID_FSW_SWITCH_LOG_EVENT .....	619
32570 - LOG_ID_ADMIN_MTNER_LOGOUT_DISCONNECT .....	620
32601 - LOG_ID_FGT_SWITCH_LOG_DISCOVER .....	621
32602 - LOG_ID_FGT_SWITCH_LOG_AUTH .....	622
32603 - LOG_ID_FGT_SWITCH_LOG_DEAUTH .....	623
32604 - LOG_ID_FGT_SWITCH_LOG_DELETE .....	623
32605 - LOG_ID_FGT_SWITCH_LOG_TUNNEL_UP .....	624
32606 - LOG_ID_FGT_SWITCH_LOG_TUNNEL_DOWN .....	625
32607 - LOG_ID_FGT_SWITCH_PUSH_IMAGE .....	626
32608 - LOG_ID_FGT_SWITCH_STAGE_IMAGE .....	627
32609 - LOG_ID_FGT_SWITCH_DISABLE_DISCOVERY .....	627
32610 - LOG_ID_FGT_SWITCH_LOG_WARNING .....	628
32611 - LOG_ID_FGT_SWITCH_EXPORT_POOL .....	629
32612 - LOG_ID_FGT_SWITCH_EXPORT_VDOM .....	630
32613 - LOG_ID_FGT_SWITCH_REQUEST_PORT .....	630
32614 - LOG_ID_FGT_SWITCH_RETURN_PORT .....	631
32615 - LOG_ID_FGT_SWITCH_MAC_ADD .....	632
32616 - LOG_ID_FGT_SWITCH_MAC_DEL .....	633
32617 - LOG_ID_FGT_SWITCH_MAC_MOVE .....	634
32693 - LOG_ID_FGT_SWITCH_GROUP_SWC .....	634
32694 - LOG_ID_FGT_SWITCH_GROUP_POE .....	635
32695 - LOG_ID_FGT_SWITCH_GROUP_LINK .....	636
32696 - LOG_ID_FGT_SWITCH_GROUP_STP .....	637
32697 - LOG_ID_FGT_SWITCH_GROUP_SWITCH .....	638
32698 - LOG_ID_FGT_SWITCH_GROUP_ROUTER .....	639
32699 - LOG_ID_FGT_SWITCH_GROUP_SYSTEM .....	640
32700 - LOG_ID_DPDK_EARLY_INIT_FAIL .....	641

34415 - LOG_ID_NP6_IPSEC_ENGINE_BUSY .....	642
34416 - LOG_ID_NP6_IPSEC_ENGINE_POSSIBLY_LOCKUP .....	642
34417 - LOG_ID_NP6_IPSEC_ENGINE_LOCKUP .....	643
34418 - LOG_ID_NP6_HPE_PACKET_DROP .....	644
34419 - LOG_ID_NP6_HPE_PACKET_FLOOD .....	644
34428 - LOG_ID_NP7_HPE_PACKET_DROP .....	645
34430 - LOG_ID_NP7_HPE_PACKET_FLOOD .....	646
35001 - LOG_ID_HA_SYNC_VIRDB .....	646
35002 - LOG_ID_HA_SYNC_ETDB .....	647
35003 - LOG_ID_HA_SYNC_EXDB .....	648
35004 - LOG_ID_HA_SYNC_FLDB .....	649
35005 - LOG_ID_HA_SYNC_IPS .....	649
35007 - LOG_ID_HA_SYNC_AV .....	650
35009 - LOG_ID_HA_SYNC_CID .....	651
35011 - LOG_ID_HA_SYNC_FAIL .....	651
35012 - LOG_ID_CONF_SYNC_FAIL .....	652
35013 - LOG_ID_HA_FAILOVER_FAIL .....	653
35014 - LOG_ID_HA_RESET_UPTIME .....	653
35015 - LOG_ID_HA_CLEAR_HISTORY .....	654
35016 - LOG_ID_HA_FAILOVER_SUCCESS .....	655
36881 - LOG_ID_EVENT_SYSTEM_CFG_REVERT .....	655
36882 - LOG_ID_EVENT_SYSTEM_CFG_MANUALLY_SAVED .....	656
37120 - MSGID_NEG_GENERIC_P1_NOTIF .....	657
37121 - MSGID_NEG_GENERIC_P1_ERROR .....	658
37122 - MSGID_NEG_GENERIC_P2_NOTIF .....	659
37123 - MSGID_NEG_GENERIC_P2_ERROR .....	661
37124 - MSGID_NEG_I_P1_ERROR .....	662
37125 - MSGID_NEG_I_P2_ERROR .....	663
37126 - MSGID_NEG_NO_STATE_ERROR .....	664
37127 - MSGID_NEG_PROGRESS_P1_NOTIF .....	665
37128 - MSGID_NEG_PROGRESS_P1_ERROR .....	667
37129 - MSGID_NEG_PROGRESS_P2_NOTIF .....	668
37130 - MSGID_NEG_PROGRESS_P2_ERROR .....	670
37131 - MSGID_ESP_ERROR .....	671
37132 - MSGID_ESP_CRITICAL .....	672
37133 - MSGID_INSTALL_SA .....	674
37134 - MSGID_DELETE_P1_SA .....	675
37135 - MSGID_DELETE_P2_SA .....	676
37136 - MSGID_DPD_FAILURE .....	677
37137 - MSGID_CONN_FAILURE .....	678
37138 - MSGID_CONN_UPDOWN .....	680
37139 - MSGID_P2_UPDOWN .....	681
37141 - MSGID_CONN_STATS .....	682
37889 - MSGID_VC_DELETE .....	683
37890 - MSGID_VC_MOVE_VDOM .....	684
37891 - MSGID_VC_ADD_VDOM .....	685
37892 - MSGID_VC_MOVE_MEMB_STATE .....	686
37893 - MSGID_VC_DETECT_MEMB_DEAD .....	686
37894 - MSGID_VC_DETECT_MEMB_JOIN .....	687



37895 - MSGID_VC_ADD_HADEV .....	688
37896 - MSGID_VC_DEL_HADEV .....	689
37897 - MSGID_HADEV_READY .....	690
37898 - MSGID_HADEV_FAIL .....	690
37899 - MSGID_HADEV_PEERINFO .....	691
37900 - MSGID_HBDEV_DELETE .....	692
37901 - MSGID_HBDEV_DOWN .....	693
37902 - MSGID_HBDEV_UP .....	693
37903 - MSGID_SYNC_STATUS .....	694
37904 - MSGID_HA_ACTIVITY .....	695
37907 - MSGID_VLAN_HB_UP .....	696
37908 - MSGID_VLAN_HB_DOWN .....	696
37909 - MSGID_VLAN_HB_DOWN_SUM .....	697
37910 - MSGID_HB_PACKET_LOST .....	698
37911 - MSGID_FGSP_MEMBER_JOIN .....	698
37912 - MSGID_FGSP_MEMBER_LEAVE .....	699
38010 - LOG_ID_FIPS_ENCRY_FAIL .....	700
38011 - LOG_ID_FIPS_DECRY_FAIL .....	700
38012 - LOG_ID_ENTROPY_TOKEN .....	701
38031 - LOG_ID_FSSO_LOGON .....	702
38032 - LOG_ID_FSSO_LOGOFF .....	703
38033 - LOG_ID_FSSO_SVR_STATUS .....	704
38403 - LOGID_EVENT_NOTIF_INSUFFICIENT_RESOURCE .....	705
38404 - LOGID_EVENT_NOTIF_HOSTNAME_ERROR .....	705
38405 - LOGID_NOTIF_CODE_SENDTO_SMS_PHONE .....	706
38406 - LOGID_NOTIF_CODE_SENDTO_SMS_TO .....	707
38407 - LOGID_NOTIF_CODE_SENDTO_EMAIL .....	708
38408 - LOGID_EVENT_OFTP_SSL_CONNECTED .....	708
38409 - LOGID_EVENT_OFTP_SSL_DISCONNECTED .....	709
38410 - LOGID_EVENT_OFTP_SSL_FAILED .....	710
38411 - LOGID_EVENT_TWO_F_AUTH_CODE_SENDTO .....	711
38412 - LOGID_EVENT_TOKEN_CODE_SENDTO .....	712
38420 - LOGID_EVENT_HTTPS_CONNECTION .....	712
38656 - LOGID_EVENT_RAD_RPT_PROTO_ERROR .....	713
38657 - LOGID_EVENT_RAD_RPT_PROF_NOT_FOUND .....	714
38658 - LOGID_EVENT_RAD_RPT_CTX_NOT_FOUND .....	715
38659 - LOGID_EVENT_RAD_RPT_ACCT_STOP_MISSED .....	715
38660 - LOGID_EVENT_RAD_RPT_ACCT_EVENT .....	716
38661 - LOGID_EVENT_RAD_RPT_OTHER .....	717
38662 - LOGID_EVENT_RAD_STAT_PROTO_ERROR .....	718
38663 - LOGID_EVENT_RAD_STAT_PROF_NOT_FOUND .....	718
38665 - LOGID_EVENT_RAD_STAT_ACCT_STOP_MISSED .....	719
38666 - LOGID_EVENT_RAD_STAT_ACCT_EVENT .....	720
38667 - LOGID_EVENT_RAD_STAT_OTHER .....	721
38668 - LOGID_EVENT_RAD_STAT_EP_BLK .....	722
39424 - LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_UP .....	723
39425 - LOG_ID_EVENT_SSL_VPN_USER_TUNNEL_DOWN .....	724
39426 - LOG_ID_EVENT_SSL_VPN_USER_SSL_LOGIN_FAIL .....	725
39936 - LOG_ID_EVENT_SSL_VPN_SESSION_WEB_TUNNEL_STATS .....	725

39937 - LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_DENY .....	726
39938 - LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_PASS .....	727
39939 - LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_TIMEOUT .....	728
39940 - LOG_ID_EVENT_SSL_VPN_SESSION_WEBAPP_CLOSE .....	729
39941 - LOG_ID_EVENT_SSL_VPN_SESSION_SYS_BUSY .....	730
39942 - LOG_ID_EVENT_SSL_VPN_SESSION_CERT_OK .....	731
39943 - LOG_ID_EVENT_SSL_VPN_SESSION_NEW_CON .....	732
39944 - LOG_ID_EVENT_SSL_VPN_SESSION_ALERT .....	733
39945 - LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_FAIL .....	734
39946 - LOG_ID_EVENT_SSL_VPN_SESSION_EXIT_ERR .....	735
39947 - LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_UP .....	736
39948 - LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_DOWN .....	737
39949 - LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_STATS .....	738
39950 - LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_UNKNOWNTAG .....	739
39951 - LOG_ID_EVENT_SSL_VPN_SESSION_TUNNEL_ERROR .....	740
39952 - LOG_ID_EVENT_SSL_VPN_SESSION_ENTER_CONSERVE_MODE .....	741
39953 - LOG_ID_EVENT_SSL_VPN_SESSION_LEAVE_CONSERVE_MODE .....	742
40001 - LOG_ID_PPTP_TUNNEL_UP .....	743
40002 - LOG_ID_PPTP_TUNNEL_DOWN .....	744
40003 - LOG_ID_PPTP_TUNNEL_STAT .....	745
40014 - LOG_ID_PPTP_REACH_MAX_CON .....	746
40017 - LOG_ID_L2TPD_CLIENT_CON_FAIL .....	747
40019 - LOG_ID_L2TPD_CLIENT_DISCON .....	747
40021 - LOG_ID_PPTP_NOT_CONIG .....	748
40022 - LOG_ID_PPTP_NO_IP_AVAIL .....	749
40024 - LOG_ID_PPTP_OUT_MEM .....	750
40034 - LOG_ID_PPTP_START .....	750
40035 - LOG_ID_PPTP_START_FAIL .....	751
40036 - LOG_ID_PPTP_EXIT .....	752
40037 - LOG_ID_PPTPD_SVR_DISCON .....	753
40038 - LOG_ID_PPTPD_CLIENT_CON .....	753
40039 - LOG_ID_PPTPD_CLIENT_DISCON .....	754
40101 - LOG_ID_L2TP_TUNNEL_UP .....	755
40102 - LOG_ID_L2TP_TUNNEL_DOWN .....	756
40103 - LOG_ID_L2TP_TUNNEL_STAT .....	757
40114 - LOG_ID_L2TPD_START .....	758
40115 - LOG_ID_L2TPD_EXIT .....	758
40118 - LOG_ID_L2TPD_CLIENT_CON .....	759
40704 - LOG_ID_EVENT_SYS_PERF .....	760
40705 - LOG_ID_EVENT_SYS_CPU_USAGE .....	761
40706 - LOG_ID_EVENT_SYS_BROKEN_SYMBOLIC_LINK .....	762
40960 - LOGID_EVENT_WAD_WEBPROXY_FWD_SRV_ERROR .....	763
41000 - LOG_ID_UPD_FGT_SUCC .....	763
41001 - LOG_ID_UPD_FGT_FAIL .....	764
41002 - LOG_ID_UPD_SRC_VIS .....	765
41006 - LOG_ID_UPD_FSA_VIRDB .....	765
41009 - LOG_ID_UPD_DB_SIGN_INVALID .....	766
41984 - LOG_ID_EVENT_VPN_CERT_LOAD .....	767
41985 - LOG_ID_EVENT_VPN_CERT_REMOVAL .....	768

41986 - LOG_ID_EVENT_VPN_CERT_REGEN .....	769
41987 - LOG_ID_EVENT_VPN_CERT_UPDATE .....	770
41988 - LOG_ID_EVENT_SSL_VPN_SETTING_UPDATE .....	771
41989 - LOG_ID_EVENT_VPN_CERT_ERR .....	771
41990 - LOG_ID_EVENT_VPN_CERT_UPDATE_FAILED .....	772
41991 - LOG_ID_EVENT_VPN_CERT_EXPORT .....	773
41992 - LOG_ID_EVENT_VPN_CERT_CRL_EXPIRED .....	774
42201 - LOG_ID_NETX_VMX_ATTACH .....	775
42202 - LOG_ID_NETX_VMX_DETACH .....	775
42203 - LOG_ID_NETX_VMX_DENIED .....	776
43008 - LOG_ID_EVENT_AUTH_SUCCESS .....	777
43009 - LOG_ID_EVENT_AUTH_FAILED .....	778
43010 - LOG_ID_EVENT_AUTH_LOCKOUT .....	779
43011 - LOG_ID_EVENT_AUTH_TIME_OUT .....	780
43014 - LOG_ID_EVENT_AUTH_FSAE_LOGON .....	781
43015 - LOG_ID_EVENT_AUTH_FSAE_LOGOFF .....	782
43016 - LOG_ID_EVENT_AUTH_NTLM_AUTH_SUCCESS .....	783
43017 - LOG_ID_EVENT_AUTH_NTLM_AUTH_FAIL .....	784
43018 - LOG_ID_EVENT_AUTH_FGOVRD_FAIL .....	785
43020 - LOG_ID_EVENT_AUTH_FGOVRD_SUCCESS .....	786
43025 - LOG_ID_EVENT_AUTH_PROXY_SUCCESS .....	786
43026 - LOG_ID_EVENT_AUTH_PROXY_FAILED .....	787
43027 - LOG_ID_EVENT_AUTH_PROXY_TIME_OUT .....	788
43028 - LOG_ID_EVENT_AUTH_PROXY_GROUP_INFO_FAILED .....	789
43029 - LOG_ID_EVENT_AUTH_WARNING_SUCCESS .....	790
43030 - LOG_ID_EVENT_AUTH_WARNING_TBL_FULL .....	791
43032 - LOG_ID_EVENT_AUTH_PROXY_USER_LIMIT_REACHED .....	792
43033 - LOG_ID_EVENT_AUTH_PROXY_MULTIPLE_LOGIN .....	793
43034 - LOG_ID_EVENT_AUTH_PROXY_NO_RESP .....	794
43037 - LOG_ID_EVENT_AUTH_IPV4_FLUSH .....	795
43038 - LOG_ID_EVENT_AUTH_IPV6_FLUSH .....	796
43039 - LOG_ID_EVENT_AUTH_LOGON .....	797
43040 - LOG_ID_EVENT_AUTH_LOGOUT .....	797
43041 - LOG_ID_EVENT_AUTH_DISCLAIMER_ACCEPT .....	798
43042 - LOG_ID_EVENT_AUTH_DISCLAIMER_DECLINE .....	799
43043 - LOG_ID_EVENT_AUTH_EMAIL_COLLECTING_SUCCESS .....	800
43044 - LOG_ID_EVENT_AUTH_EMAIL_COLLECTING_FAIL .....	801
43045 - LOG_ID_EVENT_AUTH_8021X_SUCCESS .....	802
43046 - LOG_ID_EVENT_AUTH_8021X_FAIL .....	803
43050 - LOG_ID_EVENT_AUTH_FSAE_CONNECT .....	804
43051 - LOG_ID_EVENT_AUTH_FSAE_DISCONNECT .....	805
43520 - LOG_ID_EVENT_WIRELESS_SYS .....	806
43521 - LOG_ID_EVENT_WIRELESS_ROGUE .....	806
43522 - LOG_ID_EVENT_WIRELESS_WTP .....	808
43524 - LOG_ID_EVENT_WIRELESS_STA .....	809
43525 - LOG_ID_EVENT_WIRELESS_ONWIRE .....	810
43526 - LOG_ID_EVENT_WIRELESS_WTPR .....	811
43527 - LOG_ID_EVENT_WIRELESS_ROGUE_CFG .....	813
43528 - LOG_ID_EVENT_WIRELESS_WTPR_ERROR .....	813

43529 - LOG_ID_EVENT_WIRELESS_CLB .....	814
43530 - LOG_ID_EVENT_WIRELESS_WIDS_WL_BRIDGE .....	815
43531 - LOG_ID_EVENT_WIRELESS_WIDS_BR_DEAUTH .....	816
43532 - LOG_ID_EVENT_WIRELESS_WIDS_NL_PBRESP .....	818
43533 - LOG_ID_EVENT_WIRELESS_WIDS_MAC_OUI .....	819
43534 - LOG_ID_EVENT_WIRELESS_WIDS_LONG_DUR .....	820
43535 - LOG_ID_EVENT_WIRELESS_WIDS_WEP_IV .....	821
43542 - LOG_ID_EVENT_WIRELESS_WIDS_EAPOL_FLOOD .....	822
43544 - LOG_ID_EVENT_WIRELESS_WIDS_MGMT_FLOOD .....	823
43546 - LOG_ID_EVENT_WIRELESS_WIDS_SPOOF_DEAUTH .....	824
43548 - LOG_ID_EVENT_WIRELESS_WIDS_ASLEAP .....	826
43550 - LOG_ID_EVENT_WIRELESS_STA_LOCATE .....	827
43551 - LOG_ID_EVENT_WIRELESS_WTP_JOIN .....	828
43552 - LOG_ID_EVENT_WIRELESS_WTP_LEAVE .....	829
43553 - LOG_ID_EVENT_WIRELESS_WTP_FAIL .....	830
43554 - LOG_ID_EVENT_WIRELESS_WTP_UPDATE .....	830
43555 - LOG_ID_EVENT_WIRELESS_WTP_RESET .....	831
43556 - LOG_ID_EVENT_WIRELESS_WTP_KICK .....	832
43557 - LOG_ID_EVENT_WIRELESS_WTP_ADD_FAILURE .....	833
43558 - LOG_ID_EVENT_WIRELESS_WTP_CFG_ERR .....	834
43559 - LOG_ID_EVENT_WIRELESS_WTP_SN_MISMATCH .....	835
43560 - LOG_ID_EVENT_WIRELESS_SYS_AC_RESTARTED .....	836
43561 - LOG_ID_EVENT_WIRELESS_SYS_AC_HOSTAPD_UP .....	837
43562 - LOG_ID_EVENT_WIRELESS_SYS_AC_HOSTAPD_DOWN .....	838
43563 - LOG_ID_EVENT_WIRELESS_ROGUE_DETECT .....	838
43564 - LOG_ID_EVENT_WIRELESS_ROGUE_OFFAIR .....	840
43565 - LOG_ID_EVENT_WIRELESS_ROGUE_ONAIR .....	841
43566 - LOG_ID_EVENT_WIRELESS_ROGUE_OFFWIRE .....	843
43567 - LOG_ID_EVENT_WIRELESS_FAKEAP_DETECT .....	844
43568 - LOG_ID_EVENT_WIRELESS_FAKEAP_ONAIR .....	846
43569 - LOG_ID_EVENT_WIRELESS_ROGUE_SUPPRESSED .....	847
43570 - LOG_ID_EVENT_WIRELESS_ROGUE_UNSUPPRESSED .....	849
43571 - LOG_ID_EVENT_WIRELESS_ROGUE_DETECT_CHG .....	850
43572 - LOG_ID_EVENT_WIRELESS_STA ASSO .....	852
43573 - LOG_ID_EVENT_WIRELESS_STA_AUTH .....	853
43574 - LOG_ID_EVENT_WIRELESS_STA_DASS .....	854
43575 - LOG_ID_EVENT_WIRELESS_STA DAUT .....	856
43576 - LOG_ID_EVENT_WIRELESS_STA_IDLE .....	857
43577 - LOG_ID_EVENT_WIRELESS_STA_DENY .....	858
43578 - LOG_ID_EVENT_WIRELESS_STA_KICK .....	859
43579 - LOG_ID_EVENT_WIRELESS_STA_IP .....	861
43580 - LOG_ID_EVENT_WIRELESS_STA_LEAVE_WTP .....	862
43581 - LOG_ID_EVENT_WIRELESS_STA_WTP_DISCONN .....	863
43582 - LOG_ID_EVENT_WIRELESS_ROGUE_CFG_UNCLASSIFIED .....	865
43583 - LOG_ID_EVENT_WIRELESS_ROGUE_CFG_ACCEPTED .....	865
43584 - LOG_ID_EVENT_WIRELESS_ROGUE_CFG_ROGUE .....	866
43585 - LOG_ID_EVENT_WIRELESS_ROGUE_CFG_SUPPRESSED .....	867
43586 - LOG_ID_EVENT_WIRELESS_WTPR_DARRP_CHAN .....	868
43587 - LOG_ID_EVENT_WIRELESS_WTPR_DARRP_START .....	869

43588 - LOG_ID_EVENT_WIRELESS_WTPR_OPER_CHAN .....	870
43589 - LOG_ID_EVENT_WIRELESS_WTPR_RADAR .....	871
43590 - LOG_ID_EVENT_WIRELESS_WTPR_NOL .....	872
43591 - LOG_ID_EVENT_WIRELESS_WTPR_COUNTRY_CFG_SUCCESS .....	874
43592 - LOG_ID_EVENT_WIRELESS_WTPR_OPER_COUNTRY .....	875
43593 - LOG_ID_EVENT_WIRELESS_WTPR_CFG_TXPOWER .....	876
43594 - LOG_ID_EVENT_WIRELESS_WTPR_OPER_TXPOWER .....	877
43595 - LOG_ID_EVENT_WIRELESS_CLB_DENY .....	878
43596 - LOG_ID_EVENT_WIRELESS_CLB_RETRY .....	879
43597 - LOG_ID_EVENT_WIRELESS_WTP_ADD .....	880
43598 - LOG_ID_EVENT_WIRELESS_WTP_ADD_XSS .....	881
43599 - LOG_ID_EVENT_WIRELESS_WTP_DEL .....	882
43600 - LOG_ID_EVENT_WIRELESS_WTPR_DARRP_STOP .....	883
43601 - LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON .....	884
43602 - LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON_SUCCESS .....	886
43603 - LOG_ID_EVENT_WIRELESS_STA_CAP_SIGNON_FAILURE .....	887
43604 - LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_REQUEST .....	888
43605 - LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_SUCCESS .....	889
43606 - LOG_ID_EVENT_WIRELESS_STA_CAP_EMAIL_FAILURE .....	891
43607 - LOG_ID_EVENT_WIRELESS_STA_CAP_DISCLAIMER_CHECK .....	892
43608 - LOG_ID_EVENT_WIRELESS_STA_CAP_DISCLAIMER_DECLINE .....	893
43609 - LOG_ID_EVENT_WIRELESS_WTPR_DARRP_OPTIMIZATION_START .....	894
43610 - LOG_ID_EVENT_WIRELESS_WTPR_DARRP_OPTIMIZATION_STOP .....	895
43611 - LOG_ID_EVENT_WIRELESS_SYS_AC_UP .....	897
43612 - LOG_ID_EVENT_WIRELESS_SYS_AC_CFG_LOADED .....	897
43613 - LOG_ID_EVENT_WIRELESS_WTP_ERR .....	898
43614 - LOG_ID_EVENT_WIRELESS_DHCP_STAVATION .....	899
43615 - LOG_ID_EVENT_WIRELESS_SYS_AC_IPSEC_FAIL .....	900
43616 - LOG_ID_EVENT_WIRELESS_WTPR_NOL_ADD .....	901
43618 - LOG_ID_EVENT_WIRELESS_WTP_IMAGE_RC_SUCCESS .....	902
43619 - LOG_ID_EVENT_WIRELESS_OFFENDINGAP_DETECT .....	903
43620 - LOG_ID_EVENT_WIRELESS_OFFENDINGAP_ONAIR .....	904
43621 - LOG_ID_EVENT_WIRELESS_WTP_DATA_CHAN_CHG .....	906
43622 - LOG_ID_EVENT_WIRELESS_WTP_VLAN_PROBE .....	907
43623 - LOG_ID_EVENT_WIRELESS_WTP_VLAN_MISSING .....	908
43624 - LOG_ID_EVENT_WIRELESS_WTP_VLAN_DETECTED .....	909
43625 - LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_SUCCESS .....	910
43626 - LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_FAILURE .....	911
43627 - LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_TIMEOUT .....	912
43628 - LOG_ID_EVENT_WIRELESS_STA_CAP_CMCC_MAC_AUTH_SUCCESS .....	914
43629 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_AUTH_FAILURE .....	915
43630 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_AUTH_SUCCESS .....	916
43631 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_AUTH_NO_RESP .....	917
43632 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_MAC_AUTH_FAILURE .....	918
43633 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_MAC_AUTH_SUCCESS .....	919
43634 - LOG_ID_EVENT_WIRELESS_STA_RADIUS_MAC_AUTH_NO_RESP .....	920
43635 - LOG_ID_EVENT_WIRELESS_STA_OKC_NO_MATCH .....	921
43636 - LOG_ID_EVENT_WIRELESS_STA_OKC_LOCAL_MATCH .....	922
43637 - LOG_ID_EVENT_WIRELESS_STA_OKC_INTER_AC_MATCH .....	924

43638 - LOG_ID_EVENT_WIRELESS_STA_OKC_INTER_AP_MATCH .....	925
43639 - LOG_ID_EVENT_WIRELESS_STA_FT_INVALID_ACTION_REQ .....	926
43640 - LOG_ID_EVENT_WIRELESS_STA_FT_INVALID_AUTH_REQ .....	927
43641 - LOG_ID_EVENT_WIRELESS_STA_FT_INVALID_REASSOC_REQ .....	928
43642 - LOG_ID_EVENT_WIRELESS_STA_FT_ACTION_REQ .....	929
43643 - LOG_ID_EVENT_WIRELESS_STA_FT_ACTION_RESP .....	930
43644 - LOG_ID_EVENT_WIRELESS_STA_FT_AUTH_REQ .....	931
43645 - LOG_ID_EVENT_WIRELESS_STA_FT_AUTH_RESP .....	932
43646 - LOG_ID_EVENT_WIRELESS_STA_FT_REASSOC_REQ .....	933
43647 - LOG_ID_EVENT_WIRELESS_STA_FT_REASSOC_RESP .....	935
43648 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_INVALID_SECOND_MSG .....	936
43649 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_INVALID_FOURTH_MSG .....	937
43650 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_FIRST_MSG .....	938
43651 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_SECOND_MSG .....	939
43652 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_THIRD_MSG .....	940
43653 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_FOURTH_MSG .....	941
43654 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_FIRST_GROUP_MSG .....	942
43655 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_SECOND_GROUP_MSG .....	943
43656 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_MAX_STA_CNT .....	944
43657 - LOG_ID_EVENT_WIRELESS_STA_ASSOC_FAIL .....	946
43658 - LOG_ID_EVENT_WIRELESS_STA_DHCP_NO_RESP .....	947
43659 - LOG_ID_EVENT_WIRELESS_STA_DHCP_DIFF_OFFER .....	948
43660 - LOG_ID_EVENT_WIRELESS_STA_DHCP_NO_ACK .....	949
43661 - LOG_ID_EVENT_WIRELESS_STA_DHCP_NAK .....	950
43662 - LOG_ID_EVENT_WIRELESS_STA_DHCP_DUP_IP .....	951
43663 - LOG_ID_EVENT_WIRELESS_STA_DHCP_DISCOVER .....	952
43664 - LOG_ID_EVENT_WIRELESS_STA_DHCP_OFFER .....	953
43665 - LOG_ID_EVENT_WIRELESS_STA_DHCP_DECLINE .....	954
43666 - LOG_ID_EVENT_WIRELESS_STA_DHCP_REQUEST .....	955
43667 - LOG_ID_EVENT_WIRELESS_STA_DHCP_ACK .....	956
43668 - LOG_ID_EVENT_WIRELESS_STA_DHCP_RELEASE .....	957
43669 - LOG_ID_EVENT_WIRELESS_STA_DHCP_INFORM .....	958
43670 - LOG_ID_EVENT_WIRELESS_STA_DHCP_SELF_ASSIGNED .....	959
43671 - LOG_ID_EVENT_WIRELESS_STA_DNS_NO_RESP .....	960
43672 - LOG_ID_EVENT_WIRELESS_STA_DNS_SERVER_FAILURE .....	961
43673 - LOG_ID_EVENT_WIRELESS_STA_DNS_NO_DOMAIN .....	962
43674 - LOG_ID_EVENT_WIRELESS_STA_WPA_KRACK_FT_REASSOC .....	963
43675 - LOG_ID_EVENT_WIRELESS_STA_AUTH_REQ .....	964
43676 - LOG_ID_EVENT_WIRELESS_STA_AUTH_RESP .....	965
43677 - LOG_ID_EVENT_WIRELESS_STA_ASSOC_REQ .....	966
43678 - LOG_ID_EVENT_WIRELESS_STA_REASSOC_REQ .....	967
43679 - LOG_ID_EVENT_WIRELESS_STA_ASSOC_RESP .....	969
43680 - LOG_ID_EVENT_WIRELESS_STA_REASSOC_RESP .....	970
43681 - LOG_ID_EVENT_WIRELESS_STA_PROBE_REQ .....	971
43682 - LOG_ID_EVENT_WIRELESS_STA_PROBE_RESP .....	972
43683 - LOG_ID_EVENT_WIRELESS_BLE_DEV_LOCATE .....	973
43684 - LOG_ID_EVENT_WIRELESS_ADDRGRP_DUPLICATE_MAC .....	974
43685 - LOG_ID_EVENT_WIRELESS_ADDRGRP_ADDR_APPLY .....	975

43686 - LOG_ID_EVENT_WIRELESS_STA_WPA_MSG_INVALID_SCHEDULE	975
43687 - LOG_ID_EVENT_WIRELESS_STA_WL_BRIDGE_TRAFFIC_STATS	976
43688 - LOG_ID_EVENT_WIRELESS_APCFG_RECEIVE	978
43689 - LOG_ID_EVENT_WIRELESS_APCFG_VALIDATING	978
43690 - LOG_ID_EVENT_WIRELESS_APCFG_APPLY	979
43691 - LOG_ID_EVENT_WIRELESS_APCFG_REJECT	980
43692 - LOG_ID_EVENT_WIRELESS_WTPR_ANTENNA_DEFECT_DETECT	981
43693 - LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_REQ	982
43694 - LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_RESP_ACCEPT	983
43695 - LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_RESP_REJECT	984
43696 - LOG_ID_EVENT_WIRELESS_WTPR_DRMA_START	985
43697 - LOG_ID_EVENT_WIRELESS_WTPR_DRMA_STOP	986
43698 - LOG_ID_EVENT_WIRELESS_WTPR_DRMA_MODE	988
43699 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_SOLICIT	989
43700 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_ADVERTISE	990
43701 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_REQUEST	991
43702 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_CONFIRM	992
43703 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_RENEW	993
43704 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_REPLY	994
43705 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_RELEASE	995
43706 - LOG_ID_EVENT_WIRELESS_STA_DHCP6_RECONFIGURE	996
43707 - LOG_ID_EVENT_WIRELESS_WTPR_SSID_UP	997
43708 - LOG_ID_EVENT_WIRELESS_WTPR_SSID_DOWN	998
43776 - LOG_ID_EVENT_NAC_QUARANTINE	999
43777 - LOG_ID_EVENT_NAC_ANOMALY_QUARANTINE	1000
43800 - LOG_ID_EVENT_ELBC_BLADE_JOIN	1002
43801 - LOG_ID_EVENT_ELBC_BLADE_LEAVE	1002
43802 - LOG_ID_EVENT_ELBC_MASTER_BLADE_FOUND	1003
43803 - LOG_ID_EVENT_ELBC_MASTER_BLADE_LOST	1004
43804 - LOG_ID_EVENT_ELBC_MASTER_BLADE_CHANGE	1005
43805 - LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_FOUND	1006
43806 - LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_LOST	1007
43807 - LOG_ID_EVENT_ELBC_ACTIVE_CHANNEL_CHANGE	1007
43808 - LOG_ID_EVENT_ELBC_CHASSIS_ACTIVE	1008
43809 - LOG_ID_EVENT_ELBC_CHASSIS_INACTIVE	1009
44544 - LOGID_EVENT_CONFIG_PATH	1010
44545 - LOGID_EVENT_CONFIG_OBJ	1011
44546 - LOGID_EVENT_CONFIG_ATTR	1012
44547 - LOGID_EVENT_CONFIG_OBJATTR	1012
44548 - LOGID_EVENT_CONFIG_EXEC	1013
44549 - LOGID_EVENT_CONFIG_OBJATTR_MTNER	1014
44550 - LOGID_EVENT_CONFIG_OBJ_MTNER	1015
44551 - LOGID_EVENT_CONFIG_ATTR_MTNER	1016
44552 - LOGID_EVENT_CONFIG_PATH_MTNER	1017
44553 - LOGID_EVENT_CONFIG_FIXEDPORT_DIS	1018
44554 - LOGID_EVENT_CONFIG_POL_CHANGED	1018
44555 - LOGID_EVENT_CMDB_DEADLOCK_DETECTED	1019

45057 - LOG_ID_FCC_ADD .....	1020
45058 - LOG_ID_FCC_CLOSE .....	1021
45061 - LOG_ID_FCC_CLOSE_BY_TYPE .....	1021
45071 - LOG_ID_FCC_VULN_SCAN .....	1022
45114 - LOG_ID_EC_REG_QUARANTINE .....	1023
45115 - LOG_ID_EC_REG_UNQUARANTINE .....	1024
46000 - LOG_ID_VIP_REAL_SVR_ENA .....	1025
46001 - LOG_ID_VIP_REAL_SVR_DISA .....	1026
46002 - LOG_ID_VIP_REAL_SVR_UP .....	1027
46003 - LOG_ID_VIP_REAL_SVR_DOWN .....	1028
46004 - LOG_ID_VIP_REAL_SVR_ENT_HOLDDOWN .....	1029
46005 - LOG_ID_VIP_REAL_SVR_FAIL_HOLDDOWN .....	1029
46006 - LOG_ID_VIP_REAL_SVR_FAIL .....	1030
46400 - LOG_ID_EVENT_EXT_SYS .....	1031
46401 - LOG_ID_EVENT_EXT_LOCAL .....	1032
46402 - LOG_ID_EVENT_EXT_LOCAL_ERROR .....	1032
46403 - LOG_ID_EVENT_EXT_REMOTE_EMERG .....	1033
46404 - LOG_ID_EVENT_EXT_REMOTE_ALERT .....	1034
46405 - LOG_ID_EVENT_EXT_REMOTE_CRITICAL .....	1035
46406 - LOG_ID_EVENT_EXT_REMOTE_ERROR .....	1035
46407 - LOG_ID_EVENT_EXT_REMOTE_WARNING .....	1036
46408 - LOG_ID_EVENT_EXT_REMOTE_NOTIF .....	1037
46409 - LOG_ID_EVENT_EXT_REMOTE_INFO .....	1038
46410 - LOG_ID_EVENT_EXT_REMOTE_DEBUG .....	1038
46501 - LOG_ID_INTERNAL_LTE_MODEM_DETECTION .....	1039
46502 - LOG_ID_INTERNAL_LTE_MODEM_GPSD .....	1040
46503 - LOG_ID_INTERNAL_LTE_MODEM_GPS_LOC_ACQUISITION .....	1040
46504 - LOG_ID_INTERNAL_LTE_MODEM_BILLD .....	1041
46505 - LOG_ID_INTERNAL_LTE_MODEM_BILLING_PURGED .....	1042
46506 - LOG_ID_INTERNAL_LTE_MODEM_BILLING_DAILY_LOG .....	1042
46507 - LOG_ID_INTERNAL_LTE_MODEM_FW_UPGRADE .....	1043
46508 - LOG_ID_INTERNAL_LTE_MODEM_QDL_DETECTION .....	1044
46509 - LOG_ID_INTERNAL_LTE_MODEM_REBOOT .....	1044
46510 - LOG_ID_INTERNAL_LTE_MODEM_OP_MODE .....	1045
46511 - LOG_ID_INTERNAL_LTE_MODEM_POWER_ON_OFF .....	1046
46512 - LOG_ID_INTERNAL_LTE_MODEM_SIM_STATE .....	1047
46513 - LOG_ID_INTERNAL_LTE_MODEM_LINK_CONNECTION .....	1047
46514 - LOG_ID_INTERNAL_LTE_MODEM_MANUAL_HANDOVER .....	1048
46515 - LOG_ID_INTERNAL_LTE_MODEM_IP_ADDR .....	1049
46516 - LOG_ID_INTERNAL_LTE_MODEM_BEARER_TECH_CHANGE .....	1049
46600 - LOG_ID_EVENT_AUTOMATION_TRIGGERED .....	1050
46900 - LOG_ID_POE_STATUS_REPORT .....	1051
47000 - LOG_ID_MALWARE_LIST_TRUNCATED_ENTER .....	1051
47001 - LOG_ID_MALWARE_LIST_TRUNCATED_EXIT .....	1052
47203 - LOG_ID_ENTER_BYPASS .....	1053
47204 - LOG_ID_EXIT_BYPASS .....	1053
48000 - LOG_ID_WAD_SSL_RCV_HS .....	1054
48001 - LOG_ID_WAD_SSL_RCV_WRG_HS .....	1055
48002 - LOG_ID_WAD_SSL_SENT_HS .....	1056



48003 - LOG_ID_WAD_SSL_WRG_HS_LEN .....	1057
48004 - LOG_ID_WAD_SSL_RCV_CCS .....	1058
48005 - LOG_ID_WAD_SSL_RSA_DH_FAIL .....	1059
48006 - LOG_ID_WAD_SSL_SENT_CCS .....	1060
48007 - LOG_ID_WAD_SSL_BAD_HASH .....	1061
48009 - LOG_ID_WAD_SSL_DECRY_FAIL .....	1062
48011 - LOG_ID_WAD_SSL_LESS_MINOR .....	1063
48013 - LOG_ID_WAD_SSL_NOT_SUPPORT_CS .....	1064
48016 - LOG_ID_WAD_SSL_HS_FIN .....	1065
48017 - LOG_ID_WAD_SSL_HS_TOO_LONG .....	1065
48019 - LOG_ID_WAD_SSL_SENT_ALERT .....	1066
48023 - LOG_ID_WAD_SSL_RCV_ALERT .....	1067
48027 - LOG_ID_WAD_SSL_INVALID_CONT_TYPE .....	1068
48029 - LOG_ID_WAD_SSL_BAD_CCS_LEN .....	1069
48031 - LOG_ID_WAD_SSL_BAD_DH .....	1070
48032 - LOG_ID_WAD_SSL_PUB_KEY_TOO_BIG .....	1071
48034 - LOG_ID_WAD_SSL_SERVER_KEY_HASH_ALGORITHM_MISMATCH ..	1072
48035 - LOG_ID_WAD_SSL_SERVER_KEY_SIGNATURE_ALGORITHM_	
MISMATCH .....	1073
48038 - LOG_ID_WAD_SSL_RCV_FATAL_ALERT .....	1074
48039 - LOG_ID_WAD_SSL_SENT_FATAL_ALERT .....	1075
48101 - LOG_ID_WAD_AUTH_FAIL_PSK .....	1076
48102 - LOG_ID_WAD_AUTH_FAIL_OTH .....	1077
48301 - LOG_ID_UNEXP_APP_TYPE .....	1078
49002 - LOG_ID_VNP_DPDK_PRIMARY_RESTART .....	1079
49004 - LOGID_EVENT_HYPERV_SRIOV_SHOW_UP .....	1080
49005 - LOGID_EVENT_HYPERV_SRIOV_DISAPPEAR .....	1080
51000 - LOG_ID_NB_TBL_CHG .....	1081
52000 - LOG_ID_EVENT_SECURITY_AUDIT_FABRIC_SUMMARY .....	1082
52001 - LOG_ID_EVENT_SECURITY_AUDIT_FABRIC_CHANGE .....	1083
53000 - LOG_ID_SDNC_CONNECTED .....	1084
53001 - LOG_ID_SDNC_DISCONNECTED .....	1084
53002 - LOG_ID_SDNC_SUBSCRIBE .....	1085
53003 - LOG_ID_SDNC_UNSUBSCRIBE .....	1086
53100 - LOG_ID_VPN_OCVPN_REGISTERED .....	1087
53101 - LOG_ID_VPN_OCVPN_UNREGISTERED .....	1087
53102 - LOG_ID_VPN_OCVPN_COMM_ESTABLISHED .....	1088
53103 - LOG_ID_VPN_OCVPN_COMM_ERROR .....	1089
53104 - LOG_ID_VPN_OCVPN_DNS_ERROR .....	1089
53105 - LOG_ID_VPN_OCVPN_ROUTE_ERROR .....	1090
53200 - LOG_ID_CONNECTOR_OBJECT_ADD .....	1091
53201 - LOG_ID_CONNECTOR_OBJECT_REMOVE .....	1092
53202 - LOG_ID_CONNECTOR_API_FAILED .....	1093
53203 - LOG_ID_CONNECTOR_OBJECT_UPDATE .....	1093
53204 - LOG_ID_CONNECTOR_OBJECT_CANT_ADD .....	1094
53205 - LOG_ID_CONNECTOR_OBJECT_CANT_REMOVE .....	1095
53300 - LOG_ID_VNE_PRO_UPDATE_COMPLETED .....	1096
53301 - LOG_ID_VNE_PRO_UPDATE_FAILED .....	1096
53311 - LOG_ID_NPU_PER_MAPPING_ALLOCATION .....	1097

53312 - LOG_ID_NPD_INFO .....	1098
53313 - LOG_ID_NPD_WARNING .....	1098
53314 - LOG_ID_NPD_ERROR .....	1099
FILE-FILTER .....	1100
64000 - LOG_ID_FILE_FILTER_BLOCK .....	1100
64001 - LOG_ID_FILE_FILTER_LOG .....	1102
GTP .....	1104
41216 - LOGID_GTP_FORWARD .....	1104
41217 - LOGID_GTP_DENY .....	1106
41218 - LOGID_GTP_RATE_LIMIT .....	1108
41219 - LOGID_GTP_STATE_INVALID .....	1110
41220 - LOGID_GTP_TUNNEL_LIMIT .....	1111
41221 - LOGID_GTP_TRAFFIC_COUNT .....	1113
41222 - LOGID_GTP_USER_DATA .....	1115
41223 - LOGID_GTPV2_FORWARD .....	1116
41224 - LOGID_GTPV2_DENY .....	1118
41225 - LOGID_GTPV2_RATE_LIMIT .....	1119
41226 - LOGID_GTPV2_STATE_INVALID .....	1121
41227 - LOGID_GTPV2_TUNNEL_LIMIT .....	1123
41228 - LOGID_GTPV2_TRAFFIC_COUNT .....	1124
41229 - LOGID_GTPU_FORWARD .....	1126
41230 - LOGID_GTPU_DENY .....	1127
ICAP .....	1128
60000 - LOG_ID_ICAP_SERVER_ERROR .....	1128
IPS .....	1130
16384 - LOGID_ATTCK_SIGNATURE_TCP_UDP .....	1130
16385 - LOGID_ATTCK_SIGNATURE_ICMP .....	1132
16386 - LOGID_ATTCK_SIGNATURE_OTHERS .....	1134
16399 - LOGID_ATTACK_MALICIOUS_URL .....	1136
16400 - LOGID_ATTACK_BOTNET_WARNING .....	1138
16401 - LOGID_ATTACK_BOTNET_NOTIF .....	1140
SSH .....	1143
61000 - LOG_ID_SSH_COMMAND_BLOCK .....	1143
61001 - LOG_ID_SSH_COMMAND_BLOCK_ALERT .....	1144
61002 - LOG_ID_SSH_COMMAND_PASS .....	1146
61003 - LOG_ID_SSH_COMMAND_PASS_ALERT .....	1147
61010 - LOG_ID_SSH_CHANNEL_BLOCK .....	1149
61011 - LOG_ID_SSH_CHANNEL_PASS .....	1150
SSL .....	1152
62004 - LOG_ID_SSL_EXEMPT_ADDR .....	1152
62006 - LOG_ID_SSL_EXEMPT_WHITELIST .....	1153
62007 - LOG_ID_SSL_EXEMPT_FTGD_CATEGORY .....	1155
62008 - LOG_ID_SSL_EXEMPT_LOCAL_CATEGORY .....	1156
62009 - LOG_ID_SSL_EXEMPT_USER_CATEGORY .....	1158
62100 - LOG_ID_SSL_NEGOTIATION_INSPECT .....	1159
62101 - LOG_ID_SSL_NEGOTIATION_BLOCK .....	1161
62102 - LOG_ID_SSL_NEGOTIATION_BYPASS .....	1162
62300 - LOG_ID_SSL_ANOMALY_CERT_BLACKLISTED .....	1164

62301 - LOG_ID_SSL_ANOMALY_CERT_RESIGN_TRUSTED .....	1165
62302 - LOG_ID_SSL_ANOMALY_CERT_RESIGN_UNTRUSTED .....	1167
62303 - LOG_ID_SSL_ANOMALY_CERT_BLOCKED .....	1168
62304 - LOG_ID_SSL_ANOMALY_CERT_SNI_MISMATCHED .....	1170
Traffic .....	1171
2 - LOG_ID_TRAFFIC_ALLOW .....	1171
3 - LOG_ID_TRAFFIC_DENY .....	1176
4 - LOG_ID_TRAFFIC_OTHER_START .....	1181
5 - LOG_ID_TRAFFIC_OTHER_ICMP_ALLOW .....	1186
6 - LOG_ID_TRAFFIC_OTHER_ICMP_DENY .....	1191
7 - LOG_ID_TRAFFIC_OTHER_INVALID .....	1195
8 - LOG_ID_TRAFFIC_WANOPT .....	1200
9 - LOG_ID_TRAFFIC_WEBCACHE .....	1205
10 - LOG_ID_TRAFFIC_EXPLICIT_PROXY .....	1210
11 - LOG_ID_TRAFFIC_FAIL_CONN .....	1216
12 - LOG_ID_TRAFFIC_MULTICAST .....	1220
13 - LOG_ID_TRAFFIC_END_FORWARD .....	1225
14 - LOG_ID_TRAFFIC_END_LOCAL .....	1230
15 - LOG_ID_TRAFFIC_START_FORWARD .....	1235
16 - LOG_ID_TRAFFIC_START_LOCAL .....	1240
17 - LOG_ID_TRAFFIC_SNIFFER .....	1245
19 - LOG_ID_TRAFFIC_BROADCAST .....	1250
20 - LOG_ID_TRAFFIC_STAT .....	1254
21 - LOG_ID_TRAFFIC_SNIFFER_STAT .....	1259
22 - LOG_ID_TRAFFIC_UTM_CORRELATION .....	1264
VoIP .....	1269
44032 - LOGID_EVENT_VOIP_SIP .....	1269
44033 - LOGID_EVENT_VOIP_SIP_BLOCK .....	1271
44034 - LOGID_EVENT_VOIP_SIP_FUZZING .....	1272
44035 - LOGID_EVENT_VOIP_SCCP_REGISTER .....	1274
44036 - LOGID_EVENT_VOIP_SCCP_UNREGISTER .....	1275
44037 - LOGID_EVENT_VOIP_SCCP_CALL_BLOCK .....	1276
44038 - LOGID_EVENT_VOIP_SCCP_CALL_INFO .....	1277
WAF .....	1279
30248 - LOGID_WAF_SIGNATURE_BLOCK .....	1279
30249 - LOGID_WAF_SIGNATURE_PASS .....	1281
30250 - LOGID_WAF_SIGNATURE_ERASE .....	1282
30251 - LOGID_WAF_CUSTOM_SIGNATURE_BLOCK .....	1284
30252 - LOGID_WAF_CUSTOM_SIGNATURE_PASS .....	1286
30253 - LOGID_WAF_METHOD_BLOCK .....	1288
30255 - LOGID_WAF_ADDRESS_LIST_BLOCK .....	1289
30257 - LOGID_WAF_CONSTRAINTS_BLOCK .....	1291
30258 - LOGID_WAF_CONSTRAINTS_PASS .....	1293
30259 - LOGID_WAF_URL_ACCESS_PERMIT .....	1295
30260 - LOGID_WAF_URL_ACCESS_BYPASS .....	1296
30261 - LOGID_WAF_URL_ACCESS_BLOCK .....	1298
Web .....	1300
12288 - LOG_ID_WEB_CONTENT_BANWORD .....	1300
12290 - LOG_ID_WEB_CONTENT_EXEMPTWORD .....	1302

12292 - LOG_ID_WEB_CONTENT_KEYWORD .....	1304
12293 - LOG_ID_WEB_CONTENT_SEARCH .....	1306
12544 - LOG_ID_URL_FILTER_BLOCK .....	1309
12545 - LOG_ID_URL_FILTER_EXEMPT .....	1311
12546 - LOG_ID_URL_FILTER_ALLOW .....	1313
12547 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTP_BLK .....	1315
12548 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTPS_BLK .....	1316
12549 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTP_PASS .....	1318
12550 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_HTTPS_PASS .....	1320
12551 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_SNI_BLK .....	1322
12552 - LOG_ID_URL_FILTER_INVALID_HOSTNAME_SNI_PASS .....	1324
12553 - LOG_ID_URL_FILTER_INVALID_CERT .....	1326
12554 - LOG_ID_URL_FILTER_INVALID_SESSION .....	1328
12555 - LOG_ID_URL_FILTER_SRV_CERT_ERR_BLK .....	1330
12556 - LOG_ID_URL_FILTER_SRV_CERT_ERR_PASS .....	1332
12557 - LOG_ID_URL_FILTER_FAMS_NOT_ACTIVE .....	1333
12558 - LOG_ID_URL_FILTER_RATING_ERR .....	1334
12559 - LOG_ID_URL_FILTER_PASS .....	1335
12560 - LOG_ID_URL_WISP_BLOCK .....	1337
12561 - LOG_ID_URL_WISP_REDIRECT .....	1339
12562 - LOG_ID_URL_WISP_ALLOW .....	1341
12688 - LOG_ID_WEB_SSL_EXEMPT .....	1343
12800 - LOG_ID_WEB_FTGD_ERR .....	1345
12801 - LOG_ID_WEB_FTGD_WARNING .....	1347
12802 - LOG_ID_WEB_FTGD_QUOTA .....	1349
13056 - LOG_ID_WEB_FTGD_CAT_BLK .....	1350
13057 - LOG_ID_WEB_FTGD_CAT_WARN .....	1352
13312 - LOG_ID_WEB_FTGD_CAT_ALLOW .....	1355
13315 - LOG_ID_WEB_FTGD_QUOTA_COUNTING .....	1357
13317 - LOG_ID_WEB_URL .....	1359
13568 - LOG_ID_WEB_SCRIPTFILTER_ACTIVEX .....	1361
13573 - LOG_ID_WEB_SCRIPTFILTER_COOKIE .....	1363
13584 - LOG_ID_WEB_SCRIPTFILTER_APPLET .....	1365
13600 - LOG_ID_WEB_SCRIPTFILTER_OTHER .....	1367
13601 - LOG_ID_WEB_WF_COOKIE .....	1369
13602 - LOG_ID_WEB_WF_REFERER .....	1371
13603 - LOG_ID_WEB_WF_COMMAND_BLOCK .....	1373
13616 - LOG_ID_CONTENT_TYPE_BLOCK .....	1375
13632 - LOGID_HTTP_HDR_CHG_REQ .....	1377
13633 - LOGID_HTTP_HDR_CHG_RESP .....	1379
13648 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_URL_ALLOW .....	1380
13649 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_FTGD_ALLOW .....	1382
13650 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_DEFAULT_ALLOW .....	1384
13651 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_URL_BLOCK .....	1386
13652 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_FTGD_BLOCK .....	1388
13653 - LOG_ID_WEB_WF_ANTIPHISH_MATCH_DEFAULT_BLOCK .....	1390

## Change Log

Date	Change Description
2023-06-26	Initial release.

# Introduction

This document provides information about all the log messages applicable to the FortiGate devices running FortiOS version 6.4.14 or higher. The logs are intended for administrators to use as reference for more information about a specific log entry and message generated by FortiOS.

This document also provides information about log fields when FortiOS sends log messages to remote syslog servers in Common Event Format (CEF). See [CEF Support on page 60](#). It also describes how to enable extended logging. See [UTM Extended Logging on page 71](#).



Performance statistics are not logged to disk. Performance statistics can be received by a syslog server or by FortiAnalyzer.

---

## Before you begin

Before you begin using this reference, read the following notes:

- Information in this document applies to all FortiGate units that are currently running FortiOS 6.4.14 or higher.
- Ensure that you have enabled logging for the FortiOS unit.
- Each log message is displayed in the *Log & Report* pane of the GUI. You can also download the RAW format from the *Log & Report* pane.
- Each log message is documented similar to how it appears in the RAW format.



This reference contains detailed information for each log type and subtype; however, this reference contains only information gathered at publication and, as a result, not every log message field contains detailed information.

---

## What's new

This section identifies major changes in the Log Reference from version 6.4.0 and later. For more information about new features, please see the [FortiOS 6.4 New Features Guide](#).

### FortiOS 6.4.14

There are no major log changes between FortiOS 6.4.13 and 6.4.14.

### FortiOS 6.4.13

#### Log ID changes

The following log IDs are changed.

##### Event logs:

LogID	Message	Change
20230	LOG_ID_SYS_SECURITY_WRITE_VIOLATION	Log ID Added
20231	LOG_ID_SYS_SECURITY_HARDLINK_VIOLATION	Log ID Added
20232	LOG_ID_SYS_SECURITY_LOAD_MODULE_VIOLATION	Log ID Added
20233	LOG_ID_SYS_SECURITY_FILE_HASH_MISSING	Log ID Added
20234	LOG_ID_SYS_SECURITY_FILE_HASH_MISMATCH	Log ID Added
41009	LOG_ID_UPD_DB_SIGN_INVALID	Log ID Added

### FortiOS 6.4.12

There are no major log changes between FortiOS 6.4.11 and 6.4.12.

### FortiOS 6.4.11

There are no major log changes between FortiOS 6.4.10 and 6.4.11.

### FortiOS 6.4.10

#### Log ID changes

The following log IDs are changed.

##### Event logs:

LogID	Message	Change
20027	LOG_ID_REPORT_DEL_OLD_REC	Log ID Removed
32262	LOG_ID_RESTORE_IMG_CONFIRM	Log ID Added
37911	MESGID_FGSP_MEMBER_JOIN	Log ID Added
37912	MESGID_FGSP_MEMBER_LEAVE	Log ID Added

## FortiOS 6.4.9

### Log field values

The following log field values changed.

#### Traffic logs:

Field	Change
dstreputation	Field Added
srcreputation	Field Added

### Log ID changes

The following log IDs are changed.

#### Event logs:

LogID	Message	Change
22114	LOG_ID_POWER_REDUNDANCY_DEGRADE	Log ID Added
22115	LOG_ID_POWER_REDUNDANCY_FAILURE	Log ID Added
22807	LOG_ID_VDOM_LIC	Log ID Added
32262	LOG_ID_RESTORE_IMG_CONFIRM	Log ID Added
34428	LOG_ID_NP7_HPE_PACKET_DROP	Log ID Added
34430	LOG_ID_NP7_HPE_PACKET_FLOOD	Log ID Added
38420	LOGID_EVENT_HTTPS_CONNECTION	Log ID Added
53311	LOG_ID_NPU_PER_MAPPING_ALLOCATION	Log ID Added

## FortiOS 6.4.8

There are no major log changes between FortiOS 6.4.7 and 6.4.8.



## FortiOS 6.4.7

### Log ID changes

The following log IDs are changed.

#### Event logs:

LogID	Message	Change
53312	LOG_ID_NPD_INFO	Log ID Added
53313	LOG_ID_NPD_WARNING	Log ID Added
53314	LOG_ID_NPD_ERROR	Log ID Added

## FortiOS 6.4.6

### Log ID changes

The following log IDs are changed.

#### Event logs:

LogID	Message	Change
34418	LOG_ID_NP6_HPE_PACKET_DROP	Log ID Added
34419	LOG_ID_NP6_HPE_PACKET_FLOOD	Log ID Added
43707	LOG_ID_EVENT_WIRELESS_WTPR_SSID_UP	Log ID Added
43708	LOG_ID_EVENT_WIRELESS_WTPR_SSID_DOWN	Log ID Added

## FortiOS 6.4.5

### Log ID changes

The following log IDs are changed.

#### Event logs:

LogID	Message	Change
45120	LOG_ID_EC_INVALID_EMS_TAG_REFERENCED	Log ID Removed
53203	LOG_ID_CONNECTOR_OBJECT_UPDATE	Log ID Added
53204	LOG_ID_CONNECTOR_OBJECT_CANT_ADD	Log ID Added
53205	LOG_ID_CONNECTOR_OBJECT_CANT_REMOVE	Log ID Added

## FortiOS 6.4.4

There are no major log changes between FortiOS 6.4.3 and 6.4.4.

## FortiOS 6.4.3

### Log field values

The following log field values are changed.

#### AV logs:

Field	Change
attachment	Field Added
cc	Field Added
subject	Field Added

#### DLP logs:

Field	Change
attachment	Field Added
cc	Field Added

#### Event logs:

Field	Change
operdrmamode	Field Added
slctdrmamode	Field Added
useralt	Field Added

#### FILE-FILTER logs:

Field	Change
attachment	Field Added
cc	Field Added

#### Traffic logs:

Field	Change
vwlname	Field Added

## Log ID changes

The following log IDs are changed.

### Event logs:

LogID	Message	Change
22954	LOG_ID_INET_SVC_OBSOLETE	Log ID Added
32096	LOG_ID_GUI_DOWNLOAD_LOG	Log ID Added
40706	LOG_ID_EVENT_SYS_BROKEN_SYMBOLIC_LINK	Log ID Added
43693	LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_REQ	Log ID Added
43694	LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_RESP_ACCEPT	Log ID Added
43695	LOG_ID_EVENT_WIRELESS_STA_WNM_ACTION_BSTM_RESP_REJECT	Log ID Added
43696	LOG_ID_EVENT_WIRELESS_WTPR_DRMA_START	Log ID Added
43697	LOG_ID_EVENT_WIRELESS_WTPR_DRMA_STOP	Log ID Added
43698	LOG_ID_EVENT_WIRELESS_WTPR_DRMA_MODE	Log ID Added
43699	LOG_ID_EVENT_WIRELESS_STA_DHCP6_SOLICIT	Log ID Added
43700	LOG_ID_EVENT_WIRELESS_STA_DHCP6_ADVERTISE	Log ID Added
43701	LOG_ID_EVENT_WIRELESS_STA_DHCP6_REQUEST	Log ID Added
43702	LOG_ID_EVENT_WIRELESS_STA_DHCP6_CONFIRM	Log ID Added
43703	LOG_ID_EVENT_WIRELESS_STA_DHCP6_RENEW	Log ID Added
43704	LOG_ID_EVENT_WIRELESS_STA_DHCP6_REPLY	Log ID Added
43705	LOG_ID_EVENT_WIRELESS_STA_DHCP6_RELEASE	Log ID Added
43706	LOG_ID_EVENT_WIRELESS_STA_DHCP6_RECONFIGURE	Log ID Added
53202	LOG_ID_CONNECTOR_API_FAILED	Log ID Added

## FortiOS 6.4.2

### Log field values

The following log field values are changed.

### Event logs:

Field	Change
bandwidthused	Field Added
inbandwidthused	Field Added
outbandwidthused	Field Added

**Email logs:**

Field	Change
webmailprovider	Field Added

**GTP logs:**

Field	Change
cggsn6	Field Added
cgsn6	Field Added
cpaddr6	Field Added
cpdladdr6	Field Added
cpdlisraddr6	Field Added
cpuladdr6	Field Added
csgsn6	Field Added
from6	Field Added
to6	Field Added
uggsn6	Field Added
ugsn6	Field Added
usgsn6	Field Added

**DNS logs:**

Field	Change
rcode	Field Added

**Traffic logs:**

Field	Change
dstgroup	Field Removed
tunnelid	Field Added

## Log ID changes

The following log IDs are changed.

### AV logs:

LogID	Message	Change
8981	MESGID_SCAN_AV_CDR_INTERNAL_ERROR	Log ID Added

### Event logs:

LogID	Message	Change
43692	LOG_ID_EVENT_WIRELESS_WTPR_ANTENNA_DEFECT_DETECT	Log ID Added
49002	LOG_ID_VNP_DPDK_PRIMARY_RESTART	Log ID Added
49004	LOGID_EVENT_HYPERV_SRIOV_SHOW_UP	Log ID Added
49005	LOGID_EVENT_HYPERV_SRIOV_DISAPPEAR	Log ID Added

### Email logs:

LogID	Message	Change
20480	LOGID_ANTISPAM_EMAIL_SMTP_NOTIF	Log ID Removed
20481	LOGID_ANTISPAM_EMAIL_SMTP_BWORD_NOTIF	Log ID Removed
20482	LOGID_ANTISPAM_EMAIL_POP3_NOTIF	Log ID Removed
20483	LOGID_ANTISPAM_EMAIL_POP3_BWORD_NOTIF	Log ID Removed
20484	LOGID_ANTISPAM_EMAIL_IMAP_NOTIF	Log ID Removed
20491	LOGID_ANTISPAM_EMAIL_IMAP_BWORD_NOTIF	Log ID Removed
20500	LOGID_ANTISPAM_EMAIL_MSN_NOTIF	Log ID Removed
20501	LOGID_ANTISPAM_EMAIL_YAHOO_NOTIF	Log ID Removed
20502	LOGID_ANTISPAM_EMAIL_GOOGLE_NOTIF	Log ID Removed
20503	LOGID_EMAIL_SMTP_GENERAL_NOTIF	Log ID Removed
20504	LOGID_EMAIL_POP3_GENERAL_NOTIF	Log ID Removed
20505	LOGID_EMAIL_IMAP_GENERAL_NOTIF	Log ID Removed
20506	LOGID_EMAIL_MAPI_GENERAL_NOTIF	Log ID Removed
20507	LOGID_ANTISPAM_EMAIL_MAPI_BWORD_NOTIF	Log ID Removed
20508	LOGID_ANTISPAM_EMAIL_MAPI_NOTIF	Log ID Removed
20480	LOGID_ANTISPAM_EMAIL_NOTIF	Log ID Added
20481	LOGID_EMAIL_GENERAL_NOTIF	Log ID Added

LogID	Message	Change
20482	LOGID_ANTISPAM_EMAIL_BWORD_NOTIF	Log ID Added
20510	LOGID_ANTISPAM_EMAIL_WEBMAIL_NOTIF	Log ID Added

## FortiOS 6.4.1

### Log field values

The following log field values are changed.

#### App logs:

Field	Change
parameters	Field Added

#### Event logs:

Field	Change
snr	Field Added

#### Traffic logs:

Field	Change
dstauthserver	Field Added
dstgroup	Field Added
dstuser	Field Added
signal	Field Added
snr	Field Added

### Log ID changes

The following log IDs are changed.

#### Event logs:

LogID	Message	Change
20114	LOG_ID_IPSA_SELFTEST_FAIL	Log ID Added
46516	LOG_ID_INTERNAL_LTE_MODEM_BEARER_TECH_CHANGE	Log ID Added
53300	LOG_ID_VNE_PRO_UPDATE_COMPLETED	Log ID Added
53301	LOG_ID_VNE_PRO_UPDATE_FAILED	Log ID Added

**SSL logs:**

LogID	Message	Change
62005	LOG_ID_SSL_EXEMPT_CATEGORY	Log ID Removed
62007	LOG_ID_SSL_EXEMPT_FTGD_CATEGORY	Log ID Added
62008	LOG_ID_SSL_EXEMPT_LOCAL_CATEGORY	Log ID Added
62009	LOG_ID_SSL_EXEMPT_USER_CATEGORY	Log ID Added

**FortiOS 6.4.0****Log type and subtype changes**

- Internet Content Adaptation Protocol (ICAP) is added as a new log type with a log category ID of 20.
- SD-WAN is added as a new Event log subtype.

**Log field values**

The following log field values are changed.

**Event logs:**

Field	Change
auditreporttype	Field Added
bibandwidth	Field Added
checksum	Field Removed
created	Field Added
eventtype	Field Added
hbdn_reason	Field Removed
healthcheck	Field Added
inbandwidth	Field Added
infected	Field Removed
jitter	Field Added
latency	Field Added
member	Field Added
msgproto	Field Removed
neighbor	Field Added

Field	Change
newvalue	Field Added
nf_type	Field Removed
numpassmember	Field Added
oldvalue	Field Added
outbandwidth	Field Added
packetloss	Field Added
profile_vd	Field Removed
profilegroup	Field Removed
profiletype	Field Removed
scanned	Field Removed
serviceid	Field Added
sess_duration	Field Removed
slamap	Field Added
slatargetid	Field Added
stitchaction	Field Added
suspicious	Field Removed
to	Field Removed
virus	Field Removed
waninfo	Field Added

**ICAP logs:**

Field	Change
action	Field Added
date	Field Added
devid	Field Added
dstintf	Field Added
dstintfrole	Field Added
dstip	Field Added
dstport	Field Added
eventtime	Field Added
eventtype	Field Added



Field	Change
level	Field Added
logid	Field Added
msg	Field Added
policyid	Field Added
profile	Field Added
proto	Field Added
service	Field Added
sessionid	Field Added
srcintf	Field Added
srcintfrole	Field Added
srcip	Field Added
srcport	Field Added
subtype	Field Added
time	Field Added
type	Field Added
tz	Field Added
url	Field Added
vd	Field Added

**SSL logs:**

Field	Change
certdesc	Field Added
eventsubtype	Field Added
reason	Field Removed
vrf	Field Added

**Traffic logs:**

Field	Change
counticap	Field Added
dstcity	Field Added
dstregion	Field Added
srccity	Field Added

Field	Change
srcregion	Field Added

**Web logs:**

Field	Change
antiphishdc	Field Added
antiphishrule	Field Added

**Log ID changes**

The following log IDs are changed.

**AV logs:**

Log ID	Message	Change
8457	MESGID_MMS_CHECKSUM	Log ID Removed
8458	MESGID_MMS_CHECKSUM_NOTIF	Log ID Removed

**CIFS logs:**

Log ID	Message	Change
63002	LOG_ID_CIFS_CONN_FAIL	Log ID Added
63003	LOG_ID_CIFS_AUTH_FAIL	Log ID Added
63004	LOG_ID_CIFS_AUTH_INTERNAL_ERROR	Log ID Added
63005	LOG_ID_CIFS_AUTH_KRB_ERROR	Log ID Added

**Email logs:**

LogID	Message	Change
20485	LOGID_ANTISPAM_ENDPOINT_FILTER_WARNING	Log ID Removed
20486	LOGID_ANTISPAM_ENDPOINT_FILTER_NOTIF	Log ID Removed
20487	LOGID_ANTISPAM_ENDPOINT_MM7_WARNING	Log ID Removed
20488	LOGID_ANTISPAM_ENDPOINT_MM7_NOTIF	Log ID Removed
20489	LOGID_ANTISPAM_ENDPOINT_MM1_WARNING	Log ID Removed
20490	LOGID_ANTISPAM_ENDPOINT_MM1_NOTIF	Log ID Removed
20492	LOGID_ANTISPAM_MM1_FLOOD_WARNING	Log ID Removed
20493	LOGID_ANTISPAM_MM1_FLOOD_NOTIF	Log ID Removed

LogID	Message	Change
20494	LOGID_ANTISPAM_MM4_FLOOD_WARNING	Log ID Removed
20495	LOGID_ANTISPAM_MM4_FLOOD_NOTIF	Log ID Removed
20496	LOGID_ANTISPAM_MM1_DUPE_WARNING	Log ID Removed
20497	LOGID_ANTISPAM_MM1_DUPE_NOTIF	Log ID Removed
20498	LOGID_ANTISPAM_MM4_DUPE_WARNING	Log ID Removed
20499	LOGID_ANTISPAM_MM4_DUPE_NOTIF	Log ID Removed

**Event logs:**

LogID	Message	Change
20079	LOG_ID_RAD_READY	Log ID Removed
22033	LOG_ID_FAIL_CSF_LOG_SYNC_NO_VALID_FSA	Log ID Removed
22050	LOG_ID_IPAMD_ADDRESS_ALLOCATED	Log ID Added
22051	LOG_ID_IPAMD_ADDRESS_SET_FAILED	Log ID Added
22052	LOG_ID_IPAMD_ADDRESS_INVALIDATED	Log ID Added
22053	LOG_ID_IPAMD_VALIDATION_COMPLETE	Log ID Added
22220	LOG_ID_EXT_RESOURCE	Log ID Added
22221	LOG_ID_EXT_RESOURCE_FAIL	Log ID Added
22222	LOG_ID_EXT_RESOURCE_LOAD	Log ID Added
22223	LOG_ID_EXT_RESOURCE_DEBUG	Log ID Added
22897	LOG_ID_FLCFGD_NAC_ADD	Log ID Added
22898	LOG_ID_FLCFGD_NAC_DELETE	Log ID Added
22899	LOG_ID_FLCFGD_NAC_MODIFY	Log ID Added
22919	LOG_ID_SVR_LOG_STATUS_CHANGED	Log ID Added
37910	MESGID_HB_PACKET_LOST	Log ID Added
38400	LOGID_EVENT_NOTIF_SEND_SUCC	Log ID Removed
38401	LOGID_EVENT_NOTIF_SEND_FAIL	Log ID Removed
38402	LOGID_EVENT_NOTIF_DNS_FAIL	Log ID Removed
43264	LOGID_MMS_STATS	Log ID Removed
43688	LOG_ID_EVENT_WIRELESS_APCFG_RECEIVE	Log ID Added
43689	LOG_ID_EVENT_WIRELESS_APCFG_VALIDATING	Log ID Added
43690	LOG_ID_EVENT_WIRELESS_APCFG_APPLY	Log ID Added

LogID	Message	Change
43691	LOG_ID_EVENT_WIRELESS_APCFG_REJECT	Log ID Added
45109	LOG_ID_EC_FTCL_LOGOFF	Log ID Removed
45119	LOG_ID_EC_FTCL_DISCONN	Log ID Removed
45120	LOG_ID_EC_INVALID_EMS_TAG_REFERENCED	Log ID Added
48300	LOG_ID_WRG_SVR_FGT_CONF	Log ID Removed

**ICAP logs:**

Log ID	Message	Change
60000	LOG_ID_ICAP_SERVER_ERROR	Log ID Added

**SSL logs:**

Log ID	Message	Change
62000	LOG_ID_SSL_CERT_BLACKLISTED	Log ID Removed
62001	LOG_ID_SSL_CERT_PASS	Log ID Removed
62002	LOG_ID_SSL_CERT_BLOCK	Log ID Removed
62003	LOG_ID_SSL_EXEMPT	Log ID Removed
62004	LOG_ID_SSL_EXEMPT_ADDR	Log ID Added
62005	LOG_ID_SSL_EXEMPT_CATEGORY	Log ID Added
62006	LOG_ID_SSL_EXEMPT_WHITELIST	Log ID Added
62050	LOG_ID_SSL_HS_CERT_REQ_EXEMPT	Log ID Removed
62051	LOG_ID_SSL_HS_CERT_REQ_BLOCK	Log ID Removed
62052	LOG_ID_SSL_HS_UNSUPPROTED_EXEMPT	Log ID Removed
62053	LOG_ID_SSL_HS_UNSUPPORTED_BLOCK	Log ID Removed
62100	LOG_ID_SSL_NEGOTIATION_INSPECT	Log ID Added
62101	LOG_ID_SSL_NEGOTIATION_BLOCK	Log ID Added
62102	LOG_ID_SSL_NEGOTIATION_BYPASS	Log ID Added
62200	LOG_ID_SSL_EXEMPT_ADDR	Log ID Removed
62202	LOG_ID_SSL_EXEMPT_FTGD_CAT	Log ID Removed
62300	LOG_ID_SSL_ANOMALY_CERT_BLACKLISTED	Log ID Added
62301	LOG_ID_SSL_ANOMALY_CERT_RESIGN_TRUSTED	Log ID Added
62302	LOG_ID_SSL_ANOMALY_CERT_RESIGN_UNTRUSTED	Log ID Added
62303	LOG_ID_SSL_ANOMALY_CERT_BLOCKED	Log ID Added

Log ID	Message	Change
62304	LOG_ID_SSL_ANOMALY_CERT_SNI_MISMATCHED	Log ID Added

**Web logs:**

Log ID	Message	Change
12289	LOG_ID_WEB_CONTENT_MMS_BANWORD	Log ID Removed
12291	LOG_ID_WEB_CONTENT_MMS_EXEMPTWORD	Log ID Removed
12305	LOG_ID_WEB_CONTENT_MMS_BANWORD_NOTIF	Log ID Removed
13648	LOG_ID_WEB_WF_ANTIPHISH_MATCH_URL_ALLOW	Log ID Added
13649	LOG_ID_WEB_WF_ANTIPHISH_MATCH_FTGD_ALLOW	Log ID Added
13650	LOG_ID_WEB_WF_ANTIPHISH_MATCH_DEFAULT_ALLOW	Log ID Added
13651	LOG_ID_WEB_WF_ANTIPHISH_MATCH_URL_BLOCK	Log ID Added
13652	LOG_ID_WEB_WF_ANTIPHISH_MATCH_FTGD_BLOCK	Log ID Added
13653	LOG_ID_WEB_WF_ANTIPHISH_MATCH_DEFAULT_BLOCK	Log ID Added

# Log Types and Subtypes

This section describes the log types, subtypes, and priority levels. It also describes the log field format.

## Type

Each log entry contains a Type (type) or category field that indicates its log type and which log file stores the log entry.

## Subtype

Each log entry contains a Sub Type (subtype) or subcategory field within a log type, based on the feature associated with the cause of the log entry.

For example:

- In event logs, some of the subtypes are compliance check, system, and user.
- In traffic logs, the subtypes are forward, local, multicast, and sniffer.

## List of log types and subtypes

FortiGate devices can record the following types and subtypes of log entry information:

Type	Description	Subtype
<b>Traffic</b>	Records traffic flow information, such as an HTTP/HTTPS request and its response, if any.	<ul style="list-style-type: none"><li>• FORWARD</li><li>• LOCAL</li><li>• MULTICAST</li><li>• SNIFFER</li></ul>
<b>Event</b>	Records system and administrative events, such as downloading a backup copy of the configuration, or daemon activities.	<ul style="list-style-type: none"><li>• CONNECTOR</li><li>• ENDPOINT</li><li>• FORTIEXTENDER</li><li>• HA</li><li>• ROUTER</li><li>• SDWAN</li><li>• SECURITY-RATING</li><li>• SWITCH-CONTROLLER</li><li>• SYSTEM</li></ul>

Type	Description	Subtype
		<ul style="list-style-type: none"> <li>• USER</li> <li>• VPN</li> <li>• WAD</li> <li>• WIRELESS</li> </ul>
<b>UTM</b>	Records UTM events.	See list of UTM log subtypes below

## UTM log subtypes

UTM Log Subtypes	Description	Event Type
		<ul style="list-style-type: none"> <li>• CIFS-AUTH-FAIL</li> <li>• CIFS-FILEFILTER</li> </ul>
Anomaly	Records intrusion attempts.	<ul style="list-style-type: none"> <li>• ANOMALY</li> </ul>
App	Records intrusion attempts. Application control log is output when a signature matches an application pattern.	<ul style="list-style-type: none"> <li>• PORT-VIOLATION</li> <li>• PROTOCOL-VIOLATION</li> <li>• SIGNATURE</li> </ul>
AV	Records virus attacks.	<ul style="list-style-type: none"> <li>• ANALYTICS</li> <li>• COMMAND-BLOCKED</li> <li>• CONTENT-DISARM</li> <li>• FILENAME</li> <li>• FILETYPE-EXECUTABLE</li> <li>• INFECTED</li> <li>• MALWARE-LIST</li> <li>• MIMEFRAGMENTED</li> <li>• OUTBREAK-PREVENTION</li> <li>• OVERSIZE</li> <li>• SCANERROR</li> <li>• SWITCHPROTO</li> </ul>
DLP	Records data leak prevention events.	<ul style="list-style-type: none"> <li>• DLP</li> <li>• DLP-DOCSOURCE</li> </ul>
DNS	Records domain name server events.	<ul style="list-style-type: none"> <li>• DNS-QUERY</li> <li>• DNS-RESPONSE</li> </ul>
Email	Records email filter events.	<ul style="list-style-type: none"> <li>• BANNEDWORD</li> <li>• EMAIL</li> <li>• FTGD_ERR</li> <li>• SPAM</li> </ul>

UTM Log Subtypes	Description	Event Type
		<ul style="list-style-type: none"> <li>• WEBMAIL</li> </ul>
FILE-FILTER	Records file filter events.	<ul style="list-style-type: none"> <li>• FILE-FILTER</li> </ul>
GTP	Records GTP events.	<ul style="list-style-type: none"> <li>• GTP-ALL</li> </ul>
ICAP	Records ICAP events.	<ul style="list-style-type: none"> <li>• ICAP</li> </ul>
IPS	Records intrusion prevention events.	<ul style="list-style-type: none"> <li>• BOTNET</li> <li>• MALICIOUS-URL</li> <li>• SIGNATURE</li> </ul>
SSH	Records Secure Socket Shell events.	<ul style="list-style-type: none"> <li>• SSH-CHANNEL</li> <li>• SSH-COMMAND</li> </ul>
SSL	Records detected/blocked malicious SSL connections.	<ul style="list-style-type: none"> <li>• SSL-ANOMALIES</li> <li>• SSL-EXEMPT</li> <li>• SSL-NEGOTIATION</li> </ul>
VoIP	Records voice over IP events.	<ul style="list-style-type: none"> <li>• VOIP</li> </ul>
WAF	Records web application firewall information for FortiWeb appliances and virtual appliances.	<ul style="list-style-type: none"> <li>• WAF-ADDRESS-LIST</li> <li>• WAF-CUSTOM-SIGNATURE</li> <li>• WAF-HTTP-CONSTRAINT</li> <li>• WAF-HTTP-METHOD</li> <li>• WAF-SIGNATURE</li> <li>• WAF-URL-ACCESS</li> </ul>
Web	Records web filter events.	<ul style="list-style-type: none"> <li>• ACTIVEXFILTER</li> <li>• ANTIPHISHING</li> <li>• APPLETFILTER</li> <li>• CONTENT</li> <li>• COOKIEFILTER</li> <li>• FTGD_ALLOW</li> <li>• FTGD_BLK</li> <li>• FTGD_ERR</li> <li>• FTGD_QUOTA</li> <li>• FTGD_QUOTA_COUNTING</li> <li>• FTGD_QUOTA_EXPIRED</li> <li>• HTTP_HEADER_CHANGE</li> <li>• SCRIPTFILTER</li> <li>• SSL-EXEMPT</li> <li>• URLFILTER</li> <li>• URLMONITOR</li> <li>• WEBFILTER_COMMAND_BLOCK</li> </ul>



## FortiOS priority levels

Each log entry contains a Level (level) field that indicates the estimated severity of the event that caused the log entry, such as `level=warning`, and therefore how high a priority it is likely to be. Level (level) associations with the descriptions below are not always uniform. They also may not correspond with your own definitions of how severe each event is. If you require notification when a specific event occurs, either configure SNMP traps or alert email by administrator-defined Severity Level (severity\_level) or ID (logid), not by Level (level).

Level (0 is highest)	Name	Description
0	Emergency	The system is unusable or not responding.
1	Alert	Immediate action required. Used in security logs.
2	Critical	Functionality is affected.
3	Error	An error exists and functionality could be affected.
4	Warning	Functionality could be affected.
5	Notification	Information about normal events.
6	Information	General information about system operations. Used in event logs to record configuration changes.

For each location where the FortiGate device can store log files (disk, memory, Syslog or FortiAnalyzer), you can define a severity threshold. FortiOS stores all log messages equal to or exceeding the log severity level selected. For example, if you select Error, FortiOS will store log messages whose log severity level is Error, Critical, Alert, and Emergency.

## Log field format

The following table describes the standard format in which each log type is described in this document. For documentation purposes, all log types and subtypes follow this generic table format to present the log entry information.

Log Field Name	Description	Data Type	Length
appact	The security action from app control	string	16

# Log Schema Structure

This section describes the schema of the FortiOS log messages.

## Log message fields

Each log message consists of several sections of fields. In the FortiOS GUI, you can view the logs in the *Log & Report* pane, which displays the formatted view. If you want to view logs in raw format, you must download the log and view it in a text editor.

Following is an example of a traffic log message in raw format:

```
date=2017-11-15 time=11:44:16 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1510775056 srcip=10.1.100.155 srcname="pc1"
srcport=40772 srcintf="port12" srcintfrole="undefined" dstip=35.197.51.42
dstname="fortiguard.com" dstport=443 dstintf="port11" dstintfrole="undefined"
poluuid="707a0d88-c972-51e7-bbc7-4d421660557b" sessionid=8058 proto=6 action="close"
policyid=1 policytype="policy" policymode="learn" service="HTTPS" dstcountry="United
States" srccountry="Reserved"trandisp="snat" transip=172.16.200.2 transport=40772
appid=40568 app="HTTPS.BROWSER" appcat="Web.Client" apprisk="medium" duration=2
sentbyte=1850 rcvdbyte=39898 sentpkt=25 rcvpkt=37 utmaction="allow" countapp=1
devtype="Linux PC" oiname="Linux" mastersrcmac="a2:e9:00:ec:40:01"
srcmac="a2:e9:00:ec:40:01" srcserver=0 utmref=0-220586
```

The following table provides an example of the log field information in the FortiOS GUI in the detailed view of the *Log & Report* pane and in the downloaded, raw log file.

GUI Field Name (Raw Field Name)	Field Description	Example Field Value in Raw Format
<b>General</b>		
Date (date)	Day, month, and year when the log message was recorded.	date=2017-11-15
Direction (direction)	Indicates message/packets direction.	direction=incoming
Time (time)	Hour clock when the log message was recorded.	time=11:44:16
Duration (seconds)	Duration of the session, in seconds.	duration=2
Session ID (sessionid)	ID for the session.	sessionid=8058
Virtual Domain (vd)	Name of the virtual domain in which the log message was recorded.	vd="vdom1"

GUI Field Name (Raw Field Name)	Field Description	Example Field Value in Raw Format
NAT Translation (transport)	NAT source port.	transport=40772
<b>Source</b>		
IP (srcip)	IP address of the traffic's origin. The source varies by the direction: <ul style="list-style-type: none"> <li>In HTTP requests, this is the web browser or other client.</li> <li>In HTTP responses, this is the physical server.</li> </ul>	srcip=10.1.100.155
NAT IP (transip)	NAT source IP.	transip=172.16.200.2
Source Port (srcport)	Port number of the traffic's origin.	srcport=40772
Country (srccountry)	Name of the source country.	srccountry="Reserved"
Source Interface(srcintf)	Interface name of the traffic's origin.	srcintf="port12"
Source Name (srcname)	Name of the source.	srcname="pc1"
Source Interface Name (srcintfrole)	Name of the source interface.	srcintfrole="undefined"
Device Type (devtype)	Device type of the source.	devtype="Linux PC"
OS Name (osname)	OS of the source.	osname="Linux"
Master Source MAC (mastersrcmac)	The master MAC address for a host that has multiple network interfaces.	mastersrcmac="a2:e9:00:ec:40:01"
Source MAC (srcmac)	MAC address associated with the source IP address.	srcmac="a2:e9:00:ec:40:01"
Source Server (srcserver)	Server of the source.	srcserver=0
Device ID (devid)	Serial number of the device for the traffic's origin.	devid="FGVM02Q105060010"
<b>Destination</b>		
IP (dstip)	Destination IP address for the web.	dstip=35.197.51.42
Port (dstport)	Port number of the traffic's destination.	dstport=443
Country (dstcountry)	Name of the destination country.	dstcountry="United States"
Destination Interface (dstintf)	Interface of the traffic's destination.	dstintf="port11"

GUI Field Name (Raw Field Name)	Field Description	Example Field Value in Raw Format
Destination Name (dstname)	Name of the destination.	dstname="fortiguard.com"
Destination Interface Name (dstinfole)	Name of the destination interface.	dstinfole="undefined"
<b>Application</b>		
Application Name (app)	Name of the application.	app="HTTPS.BROWSER"
Category (appcat)	Category of the application.	appcat="Web.Client"
Service (service)	Name of the service.	service="HTTPS"
Application ID (appid)	ID of the application.	appid=40568
Application Risk (apprisk)	Risk level of the application.	apprisk="medium"
countapp	Number of App Ctrl logs associated with the session.	countapp=1
<b>Data</b>		
Received bytes (rcvdbyte)	Number of bytes received.	rcvdbyte=39898
Received packets (rcvdpkt)	Number of packets received.	rcvdpkt=37
Sent bytes (sentbyte)	Number of bytes sent.	sentbyte=1850
Sent packets (sentpkt)	Number of packets sent.	sentpkt=25
<b>Action</b>		
Action (action)	Status of the session. Uses following definitions: <ul style="list-style-type: none"> <li>Deny: blocked by firewall policy</li> <li>Start: session start log (special option to enable logging at start of a session). This means firewall allowed.</li> <li>All Others: allowed by Firewall Policy and the status indicates how it was closed.</li> </ul>	action=close
Policy (policyid)	Name of the firewall policy governing the traffic which caused the log message.	policyid=1
Policy UUID (poluuid)	UUID for the firewall policy.	poluuid="707a0d88-c972-51e7-bbc7-4d421660557b"

GUI Field Name (Raw Field Name)	Field Description	Example Field Value in Raw Format
Policy Type (policytype)		policytype="policy"
Policy Mode (policymode)	Firewall policy mode.	policymode="learn"
<b>Security</b>		
Level (level)	Security level rating.	level="notice"
<b>Other</b>		
Event Time (eventtime)	Epoch time the log was triggered by FortiGate. If you convert the epoch time to human readable time, it might not match the Date and Time in the header owing to a small delay between the time the log was triggered and recorded. The Log Time field is the same for the same log among all log devices, but the Date and Time might differ.	eventtime=1510775056
Protocol Number (proto)	tcp: The protocol used by web traffic (tcp by default)	proto=6
Type (type)	Log type. See <a href="#">Type on page 46</a>	type="traffic"
Log ID (logid)	Log ID. See <a href="#">Log ID definitions on page 54</a>	logid="0000000013"
Sub Type(subtype)	Subtype of the traffic. See <a href="#">Subtype on page 46</a> .	subtype="forward"
trandisp	NAT translation type.	trandisp="snat"
UTM Action (utmaction)	Security action performed by UTM.	utmaction="allow"
UTM Reference (utmref)	UTM reference number.	utmref=0-220586
UTM Reference (utmref)	UTM reference number.	utmref=0-220586

## Log ID numbers

The ID (logid) is a 10-digit field. It is a unique identifier for that specific log and includes the following information about the log entry.

Log ID number components	Description	Examples
Log Type	Represented by the first two digits of the log ID.	<ul style="list-style-type: none"> <li>Traffic log IDs begin with "00".</li> <li>Event log IDs begin with "01".</li> </ul>
Sub Type or Event Type	Represented by the second two digits of the log ID.	<ul style="list-style-type: none"> <li>VPN log subtype is represented with "01" which belongs to the Event log type that is represented with "01". Therefore, all VPN related Event log IDs will begin with the 0101 log ID series.</li> </ul>
Message ID	The last six digits of the log ID represent the message ID.	<ul style="list-style-type: none"> <li>An administrator account always has the log ID 0000003401.</li> </ul>

The logid field is a number assigned to all permutations of the same message. It classifies a log entry by the nature of the cause of the log message, such as administrator authentication failures or traffic. Other log messages that share the same cause will share the same logid.

## Log ID definitions

Following are the definitions for the log type IDs and subtype IDs applicable to FortiOS:

Log Category IDs	Subtype IDs
traffic: 0	<ul style="list-style-type: none"> <li>forward: 0</li> <li>local: 1</li> <li>multicast: 2</li> <li>sniffer: 4</li> </ul>
event: 1	<ul style="list-style-type: none"> <li>system: 0</li> <li>vpn: 1</li> <li>user: 2</li> <li>router: 3</li> <li>wireless: 4</li> <li>wad: 5</li> <li>endpoint: 7</li> <li>ha: 8</li> <li>security-rating: 10</li> <li>fortiextender: 11</li> <li>connector: 12</li> <li>sdwan: 13</li> <li>switch-controller: 14</li> </ul>
voip: 2	<ul style="list-style-type: none"> <li>voip: 14</li> </ul>
av: 3	<ul style="list-style-type: none"> <li>analytics: 1</li> </ul>

Log Category IDs	Subtype IDs
	<ul style="list-style-type: none"> <li>• filetype-executable: 3</li> <li>• outbreak-prevention: 4</li> <li>• content-disarm: 5</li> <li>• command-blocked: 6</li> <li>• malware-list: 7</li> <li>• infected: 11</li> <li>• filename: 12</li> <li>• oversize: 13</li> <li>• mimefragmented: 61</li> <li>• scanerror: 62</li> <li>• switchproto: 63</li> </ul>
web: 4	<ul style="list-style-type: none"> <li>• content: 14</li> <li>• urlfilter: 15</li> <li>• ftgd_blk: 16</li> <li>• ftgd_allow: 17</li> <li>• ftgd_err: 18</li> <li>• urlmonitor: 19</li> <li>• activexfilter: 35</li> <li>• cookiefilter: 36</li> <li>• appletfilter: 37</li> <li>• ftgd_quota_counting: 38</li> <li>• ftgd_quota_expired: 39</li> <li>• ftgd_quota: 40</li> <li>• scriptfilter: 41</li> <li>• webfilter_command_block: 43</li> <li>• http_header_change: 44</li> <li>• ssl-exempt: 45</li> <li>• antiphishing: 46</li> </ul>
ips: 5	<ul style="list-style-type: none"> <li>• signature: 19</li> <li>• malicious-url: 21</li> <li>• botnet: 22</li> </ul>
anomaly: 6	<ul style="list-style-type: none"> <li>• anomaly: 20</li> </ul>
email: 7	<ul style="list-style-type: none"> <li>• email: 12</li> <li>• spam: 13</li> <li>• bannedword: 14</li> <li>• webmail: 20</li> <li>• ftgd_err: 53</li> </ul>
dlp: 8	<ul style="list-style-type: none"> <li>• dlp: 54</li> </ul>

Log Category IDs	Subtype IDs
	<ul style="list-style-type: none"> <li>• dlp-docsource: 55</li> </ul>
app: 9	<ul style="list-style-type: none"> <li>• signature: 59</li> <li>• port-violation: 60</li> <li>• protocol-violation: 61</li> </ul>
waf: 10	<ul style="list-style-type: none"> <li>• waf-signature: 0</li> <li>• waf-custom-signature: 1</li> <li>• waf-http-method: 2</li> <li>• waf-http-constraint: 3</li> <li>• waf-address-list: 4</li> <li>• waf-url-access: 5</li> </ul>
gtp: 11	<ul style="list-style-type: none"> <li>• gtp-all: 0</li> </ul>
dns: 12	<ul style="list-style-type: none"> <li>• dns-query: 0</li> <li>• dns-response: 1</li> </ul>
ssh: 13	<ul style="list-style-type: none"> <li>• ssh-command: 0</li> <li>• ssh-channel: 1</li> </ul>
ssl: 14	<ul style="list-style-type: none"> <li>• ssl-anomalies: 0</li> <li>• ssl-exempt: 1</li> <li>• ssl-negotiation: 2</li> </ul>
: 15	<ul style="list-style-type: none"> <li>• cifs-filefilter: 0</li> <li>• cifs-auth-fail: 1</li> </ul>
file-filter: 16	<ul style="list-style-type: none"> <li>• file-filter: 0</li> </ul>
icap: 17	<ul style="list-style-type: none"> <li>• icap: 0</li> </ul>



# FortiGuard Web Filter Categories

The below details the mapping between FortiGuard Web Filter category names and numbers.

Number	Category
0	Unrated
1	Drug abuse
2	Alternative beliefs
3	Hacking
4	Illegal or unethical
5	Discrimination
6	Explicit violence
7	Abortion
8	Other adult materials
9	Advocacy organizations
11	Gambling
12	Extremist groups
13	Nudity and risque
14	Pornography
15	Dating
16	Weapons (sales)
17	Advertising
18	Brokerage and trading
19	Freeware and software downloads
20	Games
23	Web-based email
24	File sharing and storage
25	Streaming media and download
26	Malicious websites
28	Entertainment
29	Arts and culture
30	Education

Number	Category
31	Finance and banking
33	Health and wellness
34	Job search
35	Medicine
36	News and media
37	Social networking
38	Political organizations
39	Reference
40	Global religion
41	Search engines and portals
42	Shopping
43	General organizations
44	Society and lifestyles
46	Sports
47	Travel
48	Personal vehicles
49	Business
50	Information and computer security
51	Government and legal organizations
52	Information technology
53	Armed forces
54	Dynamic content
55	Meaningless content
56	Web hosting
57	Marijuana
58	Folklore
59	Proxy avoidance
61	Phishing
62	Plagiarism
63	Sex education

Number	Category
64	Alcohol
65	Tobacco
66	Lingerie and swimsuit
67	Sports hunting and war games
68	Web chat
69	Instant messaging
70	Newsgroups and message boards
71	Digital postcards
72	Peer-to-peer file sharing
75	Internet radio and TV
76	Internet telephony
77	Child education
78	Real estate
79	Restaurant and dining
80	Personal websites and blogs
81	Secure websites
82	Content servers
83	Child abuse
84	Web-based applications
85	Domain parking
86	Spam URLs
87	Personal privacy
88	Dynamic DNS
89	Auction
90	Newly observed domain
91	Newly registered domain
92	Charitable organizations
93	Remote access
94	Web analytics
95	Online meeting

# CEF Support

You can configure FortiOS 6.4.14 to send logs to remote syslog servers in Common Event Format (CEF) by using the `config log syslogd setting command`.

When CEF is enabled, FortiOS sends logs to syslog servers in CEF. This section describes how FortiOS logs support CEF.



You can view logs in CEF on remote syslog servers or FortiAnalyzer, but not in the FortiOS GUI.

---

## FortiOS to CEF log field mapping guidelines

The following CEF format:

```
Date/Time host CEF:Version|Device Vendor|Device Product|Device Version|Signature
ID|Name|Severity| [Extension]
```

Displays as following in FortiOS logs with CEF enabled:

```
"MMM dd HH:mm:ss" "hostname of the fortigate"
CEF:0|Fortinet|Fortigate|version|logid|type:subtype +[eventtype] +[action] +
[status]|reversed level|...
```

The `SignatureId` field in FortiOS logs maps to the `logid` field in CEF and should be last 5 digits of `logid`.

The `Name` field in CEF uses the following formula:

```
type:subtype + [eventtype] + [action] + [status]
```

Following is an example of the header and one key-value pair for extension from the Event VPN log in CEF:

```
#Feb 12 10:31:04 syslog-800c CEF:0|Fortinet|Fortigate|v5.6.0|37127|event:vpn negotiate
success|3|FTNTFGTlogid=0101037127
```

The `type:subtype` field in FortiOS logs maps to the `cat` field in CEF.

Any fields in FortiOS logs that are unmatched to fields in CEF include the `FTNTFGT` prefix.

Quotes (") are removed from FortiOS logs to support CEF.

Forward slashes (/) in string values as well as the equal sign (=) and backward slashes (\) are escaped in FortiOS logs to support CEF.

## CEF priority levels

Following are the CEF priority levels. They are opposite of FortiOS priority levels. See also [FortiOS priority levels on page 49](#).

Level (8 is highest)	Name	Description
8	Emergency	The system is unusable or not responding.
7	Alert	Immediate action required. Used in security logs.
6	Critical	Functionality is affected.
5	Error	An error exists and functionality could be affected.
4	Warning	Functionality could be affected.
3	Notification	Information about normal events.
2	Information	General information about system operations. Used in event logs to record configuration changes.
1	Debug	Debug information.

## Examples of CEF support

This section includes examples of how the different types of log message support CEF.

### Traffic log support for CEF

The following is an example of a traffic log on the FortiGate disk:

```
date=2018-12-27 time=11:07:55 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1545937675 srcip=10.1.100.11 srcport=54190
srcintf="port12" srcintfrole="undefined" dstip=52.53.140.235 dstport=443
dstintf="port11" dstintfrole="undefined" poluuid="c2d460aa-fe6f-51e8-9505-41b5117dfdd4"
sessionid=402 proto=6 action="close" policyid=1 policytype="policy"
service="HTTPS" dstcountry="United States" srccountry="Reserved"trandisp="snat"
transip=172.16.200.1 transport=54190 appid=40568 app="HTTPS.BROWSER"
appcat="Web.Client" apprisk="medium" applist="g-default" duration=2 sentbyte=3652
rcvdbyte=146668 sentpkt=58 rcvdpkt=105 utmaction="allow" countapp=2 utmref=65532-56
```

The following is an example of a traffic log sent in CEF format to a syslog server:

```
Dec 27 11:07:55 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|00013|traffic:forward
close|3|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0000000013
cat=traffic:forward FTNTFGTsubtype=forward FTNTFGTlevel=notice FTNTFGTvd=vdom1
FTNTFGTeventtime=1545937675 src=10.1.100.11 spt=54190 deviceInboundInterface=port12
FTNTFGTsrcintfrole=undefined dst=52.53.140.235 dpt=443
deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined FTNTFGTpoluuid=c2d460aa-
fe6f-51e8-9505-41b5117dfdd4 externalId=402 proto=6 act=close FTNTFGTpolicyid=1
FTNTFGTpolicytype=policy app=HTTPS FTNTFGTdstcountry=United States
FTNTFGTsrccountry=Reserved FTNTFGTtrandisp=snat sourceTranslatedAddress=172.16.200.1
sourceTranslatedPort=54190 FTNTFGTappid=40568 FTNTFGTapp=HTTPS.BROWSER
FTNTFGTappcat=Web.Client FTNTFGTapprisk=medium FTNTFGTapplist=g-default
FTNTFGTduration=2 out=3652 in=146668 FTNTFGTsentpkt=58 FTNTFGTrcvdpkt=105
FTNTFGTutmaction=allow FTNTFGTcountapp=2
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
type: subtype	cat
srcip	src
srcport	spt
srcintf	deviceInboundInterface
dstip	dst
dstport	dpt
dstintf	deviceOutboundInterface
sessionid	externalID
proto	proto
action	act
transip	sourceTranslatedAddress
transport	sourceTranslatedPort
service	app
sentbyte	out
rcvdbyte	in

## Custom fields

To configure the traffic log with custom fields, enter the following CLI commands:

```
config log custom-field
  edit 1
    set name "custom_name1"
    set value "HN123456"
  next
  edit 2
    set name "custom_name2"
    set value "accounting_dpt"
  next
end
config firewall policy
  edit 1
    set name "A-v4-out"
    set srcintf "port12"
    set dstintf "port11"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set logtraffic all
    set custom-log-fields "1" "2"
```

```

set application-list "g-default"
set ssl-ssh-profile "certificate-inspection"
set nat enable
next
end

```

The following is an example of a traffic log with custom fields on the FortiGate disk:

```

date=2018-12-27 time=11:12:30 logid="0000000013" type="traffic" subtype="forward"
level="notice" vd="vdom1" eventtime=1545937950 srcip=10.1.100.11 srcport=58843
srcintf="port12" srcintfrole="undefined" dstip=172.16.200.55 dstport=53
dstintf="port11" dstintfrole="undefined" poluid="c2d460aa-fe6f-51e8-9505-41b5117dfdd4"
sessionid=440 proto=17 action="accept" policyid=1 policytype="policy"
service="DNS" dstcountry="Reserved" srccountry="Reserved" trandisp="snat"
transip=172.16.200.1 transport=58843 appid=16195 app="DNS" appcat="Network.Service"
apprisk="elevated" applist="g-default" duration=180 sentbyte=70 rcvbyte=528
sentpkt=1 rcvdpkt=1 custom_name1="HN123456" custom_name2="accounting_dpt"

```

The following is an example of a traffic log with custom fields sent in CEF format to a syslog server:

```

Dec 27 11:12:30 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|00013|traffic:forward
accept|3|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0000000013
cat=traffic:forward FTNTFGTsubtype=forward FTNTFGTlevel=notice FTNTFGTvd=vdom1
FTNTFGTeventtime=1545937950 src=10.1.100.11 spt=58843 deviceInboundInterface=port12
FTNTFGTsrcintfrole=undefined dst=172.16.200.55 dpt=53 deviceOutboundInterface=port11
FTNTFGTdstintfrole=undefined FTNTFGTpoluid=c2d460aa-fe6f-51e8-9505-41b5117dfdd4
externalId=440 proto=17 act=accept FTNTFGTpolicyid=1 FTNTFGTpolicytype=policy
app=DNS FTNTFGTdstcountry=Reserved FTNTFGTsrccountry=Reserved FTNTFGTtrandisp=snat
sourceTranslatedAddress=172.16.200.1 sourceTranslatedPort=58843 FTNTFGTappid=16195
FTNTFGTapp=DNS FTNTFGTappcat=Network.Service FTNTFGTapprisk=elevated
FTNTFGTapplist=g-default FTNTFGTduration=180 out=70 in=528 FTNTFGTsentpkt=1
FTNTFGTrcvdpkt=1 FTNTFGTcustom_name1=HN123456 FTNTFGTcustom_name2=accounting_dpt

```

The following table maps FortiOS custom log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
custom_name1	FTNTFGTcustom_name1
custom_name2	FTNTFGTcustom_name2

## Event log support for CEF

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
msg	msg
cookies	requestCookies
user	duser
status	outcome
role	sourceServiceName
ui	sproc

FortiOS Log Field Name	CEF Field Name
reason	reason
action	act

## system subtype

The following is an example of a system subtype event log on the FortiGate disk:

```
date=2018-12-27 time=11:15:40 logid="0100032002" type="event" subtype="system"
level="alert" vd="vdom1" eventtime=1545938140 logdesc="Admin login failed" sn="0"
user="admin1" ui="https(172.16.200.254)" method="https" srcip=172.16.200.254
dstip=172.16.200.1 action="login" status="failed" reason="name_invalid"
msg="Administrator admin1 login failed from https(172.16.200.254) because of invalid
user name"
```

The following is an example of a system subtype event log sent in CEF format to a syslog server:

```
Dec 27 11:15:40 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|32002|event:system login
failed|7|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0100032002 cat=event:system
FTNTFGTsubtype=system FTNTFGTlevel=alert FTNTFGTvd=vdom1 FTNTFGTeventtime=1545938140
FTNTFGTlogdesc=Admin login failed FTNTFGTsn=0 duser=admin1 sproc=https
(172.16.200.254) FTNTFGTmethod=https src=172.16.200.254 dst=172.16.200.1 act=login
outcome=failed reason=name_invalid msg=Administrator admin1 login failed from https
(172.16.200.254) because of invalid user name
```

## user subtype

The following is an example of a user subtype log on the FortiGate disk:

```
date=2018-12-27 time=11:17:35 logid="0102043008" type="event" subtype="user"
level="notice" vd="vdom1" eventtime=1545938255 logdesc="Authentication success"
srcip=10.1.100.11 dstip=172.16.200.55 policyid=1 interface="port12" user="bob"
group="N/A" authproto="TELNET(10.1.100.11)" action="authentication" status="success"
reason="N/A" msg="User bob succeeded in authentication"
```

The following is an example of a user subtype log sent in CEF format to a syslog server:

```
Dec 27 11:17:35 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|43008|event:user
authentication success|3|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0102043008
cat=event:user FTNTFGTsubtype=user FTNTFGTlevel=notice FTNTFGTvd=vdom1
FTNTFGTeventtime=1545938255 FTNTFGTlogdesc=Authentication success src=10.1.100.11
dst=172.16.200.55 FTNTFGTpolicyid=1 deviceInboundInterface=port12 duser=bob
FTNTFGTgroup=N/A FTNTFGTauthproto=TELNET(10.1.100.11) act=authentication
outcome=success reason=N/A msg=User bob succeeded in authentication
```

## Antivirus log support for CEF

The following is an example of an antivirus log on the FortiGate disk:

```
date=2018-12-27 time=11:20:49 logid="0211008192" type="utm" subtype="virus"
eventtype="infected" level="warning" vd="vdom1" eventtime=1545938448 msg="File is
infected." action="blocked" service="HTTP" sessionid=695 srcip=10.1.100.11
dstip=172.16.200.55 srcport=44356 dstport=80 srcintf="port12"
srcintfrole="undefined" dstintf="port11" dstintfrole="undefined" policyid=1 proto=6
direction="incoming" filename="eicar.com" quarskip="File-was-not-quarantined."
```



```
virus="EICAR_TEST_FILE" dtype="Virus" ref="http://www.fortinet.com/ve?vn=EICAR_TEST_FILE" virusid=2172 url="http://172.16.200.55/virus/eicar.com" profile="g-default"
user="bob" agent="curl/7.47.0"
analyticscksum="275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabbf651fd0f"
analyticssubmit="false" crscore=50 crlevel="critical"
```

The following is an example of an antivirus log sent in CEF format to a syslog server:

```
Dec 27 11:20:48 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|08192|utm:virus infected
blocked|4|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0211008192 cat=utm:virus
FTNTFGTsubtype=virus FTNTFGTeventtype=infected FTNTFGTlevel=warning FTNTFGTvd=vdom1
FTNTFGTeventtime=1545938448 msg=File is infected. act=blocked app=HTTP
externalId=695 src=10.1.100.11 dst=172.16.200.55 spt=44356 dpt=80
deviceInboundInterface=port12 FTNTFGTsrcintfrole=undefined
deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined FTNTFGTpolicyid=1
proto=6 deviceDirection=0 fname=eicar.com FTNTFGTquarskip=File-was-not-quarantined.
FTNTFGTvirus=EICAR_TEST_FILE FTNTFGTdtype=Virus
FTNTFGTref=http://www.fortinet.com/ve?vn=EICAR_TEST_FILE FTNTFGTvirusid=2172
request=http://172.16.200.55/virus/eicar.com FTNTFGTprofile=g-default duser=bob
requestClientApplication=curl/7.47.0
FTNTFGTanalyticscksum=275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabbf651fd
0f FTNTFGTanalyticssubmit=false FTNTFGTcrscore=50 FTNTFGTcrlevel=critical
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
direction	deviceDirection (inbound/outbound mapping to 0/1)
filename	fname
ref	FTNTFGTref (There is \ added to escape = )
url	request
agent	requestClientApplication

## Webfilter log support for CEF

The following is an example of a webfilter log on the FortiGate disk:

```
date=2018-12-27 time=11:23:50 logid="0316013056" type="utm" subtype="webfilter"
eventtype="ftgd_blk" level="warning" vd="vdom1" eventtime=1545938629 policyid=1
sessionid=764 user="bob" srcip=10.1.100.11 srcport=59194 srcintf="port12"
srcintfrole="undefined" dstip=185.230.61.185 dstport=80 dstintf="port11"
dstintfrole="undefined" proto=6 service="HTTP" hostname="ambrishsriv.wixsite.com"
profile="g-default" action="blocked" reqtype="direct" url="/bizsquads" sentbyte=96
rcvbyte=0 direction="outgoing" msg="URL belongs to a denied category in policy"
method="domain" cat=26 catdesc="Malicious Websites" crscore=60 crlevel="high"
```

The following is an example of a webfilter log sent in CEF format to a syslog server:

```
Dec 27 11:23:49 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|13056|utm:webfilter ftgd_blk
blocked|4|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0316013056
cat=utm:webfilter FTNTFGTsubtype=webfilter FTNTFGTeventtype=ftgd_blk
FTNTFGTlevel=warning FTNTFGTvd=vdom1 FTNTFGTeventtime=1545938629 FTNTFGTpolicyid=1
externalId=764 duser=bob src=10.1.100.11 spt=59194 deviceInboundInterface=port12
FTNTFGTsrcintfrole=undefined dst=185.230.61.185 dpt=80
deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined proto=6 app=HTTP
dhost=ambrishsriv.wixsite.com FTNTFGTprofile=g-default act=blocked
FTNTFGTreqtype=direct request=/bizsquads out=96 in=0 deviceDirection=1 msg=URL
```

belongs to a denied category in policy FTNTFGTmethod=domain FTNTFGTcat=26  
requestContext=Malicious Websites FTNTFGTcrscore=60 FTNTFGTcrlevel=high

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
hostname	dhost
catdesc	requestContext

## IPS log support for CEF

The following is an example of an IPS log on the FortiGate disk:

```
date=2018-12-27 time=11:28:07 logid="0419016384" type="utm" subtype="ips"
eventtype="signature" level="alert" vd="vdom1" eventtime=1545938887 severity="info"
srcip=172.16.200.55 srccountry="Reserved" dstip=10.1.100.11 srcintf="port11"
srcintfrole="undefined" dstintf="port12" dstintfrole="undefined" sessionid=901
action="reset" proto=6 service="HTTP" policyid=1 attack="Eicar.Virus.Test.File"
srcport=80 dstport=44362 hostname="172.16.200.55" url="/virus/eicar.com"
direction="incoming" attackid=29844 profile="test-ips"
ref="http://www.fortinet.com/ids/VID29844" user="bob" incidentserialno=877326946
msg="file_transfer: Eicar.Virus.Test.File,"
```

The following is an example of an IPS sent in CEF format to a syslog server:

```
Dec 27 11:28:07 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|16384|utm:ips signature
reset|7|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0419016384 cat=utm:ips
FTNTFGTsubtype=ips FTNTFGTeventtype=signature FTNTFGTlevel=alert FTNTFGTvd=vdom1
FTNTFGTeventtime=1545938887 FTNTFGTseverity=info src=172.16.200.55
FTNTFGTsrccountry=Reserved dst=10.1.100.11 deviceInboundInterface=port11
FTNTFGTsrcintfrole=undefined deviceOutboundInterface=port12
FTNTFGTdstintfrole=undefined externalId=901 act=reset proto=6 app=HTTP
FTNTFGTpolicyid=1 FTNTFGTattack=Eicar.Virus.Test.File spt=80 dpt=44362
dhost=172.16.200.55 request=/virus/eicar.com deviceDirection=0 FTNTFGTattackid=29844
FTNTFGTprofile=test-ips FTNTFGTref=http://www.fortinet.com/ids/VID29844 duser=bob
FTNTFGTincidentserialno=877326946 msg=file_transfer: Eicar.Virus.Test.File,
```

## Email Spamfilter log support for CEF

The following is an example of an email spamfilter log on the FortiGate disk:

```
date=2018-12-27 time=11:36:58 logid="0508020503" type="utm" subtype="emailfilter"
eventtype="smtp" level="information" vd="vdom1" eventtime=1545939418 policyid=1
sessionid=1135 user="bob" srcip=10.1.100.11 srcport=35969 srcintf="port12"
srcintfrole="undefined" dstip=172.18.62.158 dstport=25 dstintf="port11"
dstintfrole="undefined" proto=6 service="SMTP" profile="test-spam" action="log-only"
from="testpcl@qa.fortinet.com" to="test1@server88.qa.fortinet.com"
sender="testpcl@qa.fortinet.com" recipient="test1@server88.qa.fortinet.com"
direction="outgoing" msg="general email log" subject="hello_world2" size="216"
attachment="no"
```

The following is an example of an email spamfilter log sent in CEF format to a syslog server:

```
Dec 27 11:36:58 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|20503|utm:emailfilter smtp
log-only|2|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0508020503
cat=utm:emailfilter FTNTFGTsubtype=emailfilter FTNTFGTeventtype=smtp
FTNTFGTlevel=information FTNTFGTvd=vdom1 FTNTFGTeventtime=1545939418
```

```
FTNTFGTpolicyid=1 externalId=1135 duser=bob src=10.1.100.11 spt=35969
deviceInboundInterface=port12 FTNTFGTsrcintfrole=undefined dst=172.18.62.158 dpt=25
deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined proto=6 app=SMTP
FTNTFGTprofile=test-spam act=log-only suser=testpcl@qa.fortinet.com
duser=test1@server88.qa.fortinet.com FTNTFGTsender=testpcl@qa.fortinet.com
FTNTFGTrecipient=test1@server88.qa.fortinet.com deviceDirection=1 msg=general email
log FTNTFGTsubject=hello_world2 FTNTFGTsize=216 FTNTFGTattachment=no
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
from	suser
to	duser

## Anomaly log support for CEF

The following is an example of an anomaly log on the FortiGate disk:

```
date=2018-12-27 time=11:40:04 logid="0720018433" type="utm" subtype="anomaly"
eventtype="anomaly" level="alert" vd="vdom1" eventtime=1545939604
severity="critical" srcip=10.1.100.11 srccountry="Reserved" dstip=172.16.200.55
srcintf="port12" srcintfrole="undefined" sessionid=0 action="clear_session" proto=1
service="PING" count=1 attack="icmp_flood" icmpid="0x3053" icmptype="0x08"
icmpcode="0x00" attackid=16777316 policyid=1 policytype="DoS-policy"
ref="http://www.fortinet.com/ids/VID16777316" msg="anomaly: icmp_flood, 51 >
threshold 50" crscore=50 crlevel="critical"
```

The following is an example of an anomaly log sent in CEF format to a syslog server:

```
Dec 27 11:40:04 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|18433|utm:anomaly anomaly
clear_session|7|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0720018433
cat=utm:anomaly FTNTFGTsubtype=anomaly FTNTFGTeventtype=anomaly FTNTFGTlevel=alert
FTNTFGTvd=vdom1 FTNTFGTeventtime=1545939604 FTNTFGTseverity=critical src=10.1.100.11
FTNTFGTsrccountry=Reserved dst=172.16.200.55 deviceInboundInterface=port12
FTNTFGTsrcintfrole=undefined externalId=0 act=clear_session proto=1 app=PING cnt=1
FTNTFGTattack=icmp_flood FTNTFGTicmpid=0x3053 FTNTFGTicmptype=0x08
FTNTFGTicmpcode=0x00 FTNTFGTattackid=16777316 FTNTFGTpolicyid=1
FTNTFGTpolicytype=DoS-policy FTNTFGTref=http://www.fortinet.com/ids/VID16777316
msg=anomaly: icmp_flood, 51 > threshold 50 FTNTFGTcrscore=50 FTNTFGTcrlevel=critical
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
count	cnt

## VoIP log support for CEF

The following is an example of a VoIP log on the FortiGate disk:

```
date=2018-12-27 time=16:47:09 logid="0814044032" type="utm" subtype="voip"
eventtype="voip" level="information" vd="vdom1" eventtime=1545958028 session_
id=18975 epoch=0 event_id=6857 srcip=10.1.100.11 src_port=5060 dstip=172.16.200.55
dst_port=5060 proto=17 src_int="port12" dst_int="port11" policy_id=1
profile="default" voip_proto="sip" kind="call" action="permit" status="start"
```

```
duration=0 dir="session_origin" call_id="3444-13134@127.0.0.1"
from="sip:sipp@127.0.0.1:5060" to="sip:service@172.16.200.55:5060"
```

The following is an example of an VoIP sent in CEF format to a syslog server:

```
Dec 27 16:47:08 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|44032|utm:voip voip permit
start|2|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0814044032 cat=utm:voip
FTNTFGTsubtype=voip FTNTFGTeventtype=voip FTNTFGTlevel=information FTNTFGTvd=vdom1
FTNTFGTeventtime=1545958028 externalId=18975 FTNTFGTepoch=0 FTNTFGTevent_id=6857
src=10.1.100.11 spt=5060 dst=172.16.200.55 dpt=5060 proto=17
deviceInboundInterface=port12 deviceOutboundInterface=port11 FTNTFGTpolicy_id=1
FTNTFGTprofile=default FTNTFGTvoip_proto=sip FTNTFGTkind=call act=permit
outcome=start FTNTFGTduration=0 FTNTFGTdir=session_origin FTNTFGTcall_id=3444-
13134@127.0.0.1 suser=sip:sipp@127.0.0.1:5060 duser=sip:service@172.16.200.55:5060
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
status	outcome
from	suser
to	duser

## DLP log support for CEF

The following is an example of a DLP log on the FortiGate disk:

```
date=2018-12-27 time=14:29:36 logid="0954024576" type="utm" subtype="dlp" eventtype="dlp"
level="warning" vd="vdom1" eventtime=1545949776 filteridx=1 dlpeextra="test-dlp3"
filtertype="file-type" filtercat="file" severity="medium" policyid=1 sessionid=12680
epoch=418303178 eventid=0 user="bob" srcip=10.1.100.11 srcport=33638
srcintf="port12" srcintfrole="undefined" dstip=172.18.62.158 dstport=80
dstintf="port11" dstintfrole="undefined" proto=6 service="HTTP" filetype="gif"
direction="incoming" action="block" hostname="172.18.62.158" url="/dlp/flower.gif"
agent="curl/7.47.0" filename="flower.gif" filesize=1209 profile="test-dlp"
```

The following is an example of a DLP log sent in CEF format to a syslog server:

```
Dec 27 14:29:36 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|24576|utm:dlp dlp
block|4|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=0954024576 cat=utm:dlp
FTNTFGTsubtype=dlp FTNTFGTeventtype=dlp FTNTFGTlevel=warning FTNTFGTvd=vdom1
FTNTFGTeventtime=1545949776 FTNTFGTfilteridx=1 FTNTFGTdlpeextra=test-dlp3
FTNTFGTfiltertype=file-type FTNTFGTfiltercat=file FTNTFGTseverity=medium
FTNTFGTpolicyid=1 externalId=12680 FTNTFGTepoch=418303178 FTNTFGTeventid=0 duser=bob
src=10.1.100.11 spt=33638 deviceInboundInterface=port12 FTNTFGTsrcintfrole=undefined
dst=172.18.62.158 dpt=80 deviceOutboundInterface=port11 FTNTFGTdstintfrole=undefined
proto=6 app=HTTP FTNTFGTfiletype=gif deviceDirection=0 act=block dhost=172.18.62.158
request=/dlp/flower.gif requestClientApplication=curl/7.47.0 fname=flower.gif
fsize=1209 FTNTFGTprofile=test-dlp
```

The following table maps FortiOS log field names to CEF field names.

FortiOS Log Field Name	CEF Field Name
filename	fname

## Application log support for CEF

The following is an example of an application log on the FortiGate disk:

```
date=2018-12-27 time=14:28:08 logid="1059028704" type="utm" subtype="app-ctrl"
eventtype="app-ctrl-all" level="information" vd="vdom1" eventtime=1545949688
appid=34050 srcip=10.1.100.11 dstip=104.80.89.24 srcport=56826 dstport=80
srcintf="port12" srcintfrole="undefined" dstintf="port11" dstintfrole="undefined"
proto=6 service="HTTP" direction="outgoing" policyid=1 sessionid=12567 applist="g-
default" appcat="Web.Client" app="HTTP.BROWSER_Firefox" action="pass"
hostname="detectportal.firefox.com" incidentserialno=1702350499 url="/success.txt"
msg="Web.Client: HTTP.BROWSER_Firefox," aprisk="elevated"
```

The following is an example of an application sent in CEF format to a syslog server:

```
Dec 27 14:28:08 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|28704|utm:app-ctrl app-ctrl-
all pass|2|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=1059028704 cat=utm:app-
ctrl FTNTFGTsubtype=app-ctrl FTNTFGTeventtype=app-ctrl-all FTNTFGTlevel=information
FTNTFGTvd=vdom1 FTNTFGTeventtime=1545949688 FTNTFGTappid=34050 src=10.1.100.11
dst=104.80.89.24 spt=56826 dpt=80 deviceInboundInterface=port12
FTNTFGTsrcintfrole=undefined deviceOutboundInterface=port11
FTNTFGTdstintfrole=undefined proto=6 app=HTTP deviceDirection=1 FTNTFGTpolicyid=1
externalId=12567 FTNTFGTapplist=g-default FTNTFGTappcat=Web.Client
FTNTFGTapp=HTTP.BROWSER_Firefox act=pass dhost=detectportal.firefox.com
FTNTFGTincidentserialno=1702350499 request=/success.txt msg=Web.Client:
HTTP.BROWSER_Firefox, FTNTFGTaprisk=elevated
```

## WAF log support for CEF

The following is an example of a WAF log on the FortiGate disk:

```
date=2018-12-27 time=14:55:20 logid="1203030258" type="utm" subtype="waf" eventtype="waf-
http-constraint" level="warning" vd="vdom1" eventtime=1545951320 policyid=1
sessionid=13614 user="bob" profile="waf_test" srcip=10.1.100.11 srcport=57304
dstip=172.16.200.55 dstport=80 srcintf="port12" srcintfrole="lan" dstintf="port11"
dstintfrole="wan" proto=6 service="HTTP"
url="http://172.16.200.55/index.html?a=0123456789&b=0123456789&c=0123456789"
severity="medium" action="passthrough" direction="request" agent="curl/7.47.0"
constraint="url-param-num" rawdata="Method=GET|User-Agent=curl/7.47.0"
```

The following is an example of a WAF sent in CEF format to a syslog server:

```
Dec 27 14:55:20 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|30258|utm:waf waf-http-
constraint passthrough|4|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=1203030258
cat=utm:waf FTNTFGTsubtype=waf FTNTFGTeventtype=waf-http-constraint
FTNTFGTlevel=warning FTNTFGTvd=vdom1 FTNTFGTeventtime=1545951320 FTNTFGTpolicyid=1
externalId=13614 duser=bob FTNTFGTprofile=waf_test src=10.1.100.11 spt=57304
dst=172.16.200.55 dpt=80 deviceInboundInterface=port12 FTNTFGTsrcintfrole=lan
deviceOutboundInterface=port11 FTNTFGTdstintfrole=wan proto=6 app=HTTP
request=http://172.16.200.55/index.html?a\=0123456789&b\=0123456789&c\=0123456789
FTNTFGTseverity=medium act=passthrough deviceDirection=0
requestClientApplication=curl/7.47.0 FTNTFGTconstraint=url-param-num
FTNTFGTrawdata=Method\=GET|User-Agent\=curl/7.47.0
```

## DNS log support for CEF

The following is an example of a DNS log on the FortiGate disk:

```

date=2018-12-27 time=14:45:26 logid="1501054802" type="dns" subtype="dns-response"
level="notice" vd="vdom1" eventtime=1545950726 policyid=1 sessionid=13355 user="bob"
srcip=10.1.100.11 srcport=54621 srcintf="port12" srcintfrole="lan"
dstip=172.16.200.55 dstport=53 dstintf="port11" dstintfrole="wan" proto=17
profile="default" srcmac="a2:e9:00:ec:40:01" xid=5137
qname="detectportal.firefox.com" qtype="A" qtypeval=1 qclass="IN"
ipaddr="104.80.89.26, 104.80.89.24" msg="Domain is monitored" action="pass" cat=52
catdesc="Information Technology"

```

The following is an example of an DNS sent in CEF format to a syslog server:

```

Dec 27 14:45:26 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|54802|dns:dns-response
pass|3|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=1501054802 cat=dns:dns-
response FTNTFGTsubtype=dns-response FTNTFGTlevel=notice FTNTFGTvd=vdom1
FTNTFGTeventtime=1545950726 FTNTFGTpolicyid=1 externalId=13355 duser=bob
src=10.1.100.11 spt=54621 deviceInboundInterface=port12 FTNTFGTsrcintfrole=lan
dst=172.16.200.55 dpt=53 deviceOutboundInterface=port11 FTNTFGTdstintfrole=wan
proto=17 FTNTFGTprofile=default FTNTFGTsrcmac=a2:e9:00:ec:40:01 FTNTFGTxid=5137
FTNTFGTqname=detectportal.firefox.com FTNTFGTqtype=A FTNTFGTqtypeval=1
FTNTFGTqclass=IN FTNTFGTipaddr=104.80.89.26, 104.80.89.24 msg=Domain is monitored
act=pass FTNTFGTcat=52 FTNTFGTcatdesc=Information Technology

```

## SSH log support for CEF

The following is an example of an SSH log on the FortiGate disk:

```

date=2018-12-27 time=14:36:15 logid="1600061002" type="utm" subtype="ssh" eventtype="ssh-
command" level="notice" vd="vdom1" eventtime=1545950175 policyid=1 sessionid=12921
user="bob" profile="test-ssh" srcip=10.1.100.11 srcport=56698 dstip=172.16.200.55
dstport=22 srcintf="port12" srcintfrole="lan" dstintf="port11" dstintfrole="wan"
proto=6 action="passthrough" direction="outgoing" login="root" command="ls"
severity="low"

```

The following is an example of an SSH sent in CEF format to a syslog server:

```

Dec 27 14:36:15 FGT-A-LOG CEF: 0|Fortinet|Fortigate|v6.0.3|61002|utm:ssh ssh-command
passthrough|3|deviceExternalId=FGT5HD3915800610 FTNTFGTlogid=1600061002 cat=utm:ssh
FTNTFGTsubtype=ssh FTNTFGTeventtype=ssh-command FTNTFGTlevel=notice FTNTFGTvd=vdom1
FTNTFGTeventtime=1545950175 FTNTFGTpolicyid=1 externalId=12921 duser=bob
FTNTFGTprofile=test-ssh src=10.1.100.11 spt=56698 dst=172.16.200.55 dpt=22
deviceInboundInterface=port12 FTNTFGTsrcintfrole=lan deviceOutboundInterface=port11
FTNTFGTdstintfrole=wan proto=6 act=passthrough FTNTFGTlogin=root FTNTFGTcommand=ls
FTNTFGTseverity=low

```

# UTM Extended Logging

FortiOS 6.0.0 and later supports extended logging for UTM log types to reliable Syslog servers over TCP. Extended logging adds HTTP header information to the *rawdata* field in UTM log types. You must enable extended logging before you can use the feature.

When extended logging is enabled, the following HTTP header information can be added to the *rawdata* field in UTM logs:

- Method
- X-Forwarded-For
- Request-Content-Type | Response-Content-Type
- Referer
- User-Agent

The full *rawdata* field of 20KB is only sent to reliable Syslog servers. Other logging devices, such as disk, FortiAnalyzer, and UDP Syslog servers, receive the information, but only keep a maximum of 2KB total log length, including the *rawdata* field, and discard the rest of the extended log information.

## Enabling extended logging

You can enable extended logging for the following UTM profiles:

- antivirus
- application
- dlp
- ips
- waf
- webfilter

When you enable the `extended-log` option for UTM profiles, all HTTP header information for HTTP-deny traffic is logged.

When you enable the `web-extended-all-action-log-enable` option for webfilter profile, all HTTP header information for HTTP-allow traffic is logged.

## Extended logging option in UTM profiles

The `extended-log` option has been added to all UTM profiles, for example:

```
# webfilter profile
config webfilter profile
    edit "test-webfilter"
        set extended-log enable
        set web-extended-all-action-log enable
    next
end
```

```
# av profile
config antivirus profile
  edit "av-proxy-test"
    set extended-log enable
  next
end
# waf profile
config waf profile
  edit "test-waf"
    set extended-log enable
  next
end
```

## Syslog server mode

The Syslog server mode changed to `udp`, `reliable`, and `legacy-reliable`. You must set the mode to `reliable` to support extended logging, for example:

```
config log syslogd setting
  set status enable
  set server "<ip address>"
  set mode reliable
  set facility local6
end
```

## Example of an extended log

Following is an example extended log for a `utm` log type with a `webfilter` subtype for a reliable Syslog server. The `rawdata` field contains the extended log data.

```
Dec 18 15:40:15 10.6.30.254 date=2017-12-18 time=15:40:14 devname="600D-9"
devid="FGT6HD3915800120" logid="0316013056" type="utm" subtype="webfilter"
eventtype="ftgd_blk" level="warning" vd="vdom1" eventtime=1513640414 policyid=2
sessionid=440522 srcip=10.1.100.128 srcport=60995 srcintf="port2" srcintfrole="lan"
dstip=209.121.139.177 dstport=80 dstintf="port1" dstintfrole="wan" proto=6
service="HTTP" hostname="detectportal.firefox.com" profile="test-webfilter"
action="blocked" reftype="direct" url="/success.txt" sentbyte=285 rcvbyte=0
direction="outgoing" msg="URL belongs to a denied category in policy"
method="domain" cat=52 catdesc="Information Technology" crscore=30 crlevel="high"
rawdata="Method=GET|User-Agent=Mozilla/5.0 (Windows NT 6.1; rv:57.0) Gecko/20100101
Firefox/57.0"
```



# Log Messages

The following sections list the FortiOS 6.4.13 log messages by log ID number.

## Anomaly

### 18432 - LOGID\_ATTCK\_ANOMALY\_TCP\_UDP

**Message ID:** 18432

**Message Description:** LOGID\_ATTCK\_ANOMALY\_TCP\_UDP

**Message Meaning:** Attack detected by UCP/TCP anomaly

**Type:** Anomaly

**Category:** ANOMALY

**Severity:** Alert

Log Field Name	Description	Data Type	Length
action	Action	string	16
attack	Attack	string	256
attackid	Attack ID	uint32	10
count	Count	uint32	10
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Deivce ID	string	16
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32

Log Field Name	Description	Data Type	Length
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log Message	string	518
policyid	Policy ID	uint32	10
policytype	Policy type	string	24
proto	Protocol	uint8	3
ref	Reference	string	4096
service	Name of Service	string	80
sessionid	Session ID	uint32	10
severity	Severity	string	8
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User	string	256
vd	Virtual Domain Name	string	32
vrf	Virtual router forwarding	uint8	3

## 18433 - LOGID\_ATTCK\_ANOMALY\_ICMP

**Message ID:** 18433

**Message Description:** LOGID\_ATTCK\_ANOMALY\_ICMP

**Message Meaning:** Attack detected by ICMP anomaly

**Type:** Anomaly**Category:** ANOMALY**Severity:** Alert

Log Field Name	Description	Data Type	Length
action	Action	string	16
attack	Attack	string	256
attackid	Attack ID	uint32	10
count	Count	uint32	10
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
eventtime	Time when detection occurred	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log Message	string	518
policyid	Policy ID	uint32	10
policytype	Policy type	string	24
proto	Protocol	uint8	3
ref	Reference	string	4096
service	Name of Service	string	80
sessionid	Session ID	uint32	10
severity	Severity	string	8
srccountry	Country name for Source IP	string	64
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User	string	256
vd	Virtual Domain Name	string	32
vrf	Virtual router forwarding	uint8	3
icmpcode	ICMP code	string	6
icmpid	ICMP ID	string	8
icmptype	ICMP Type	string	6

## 18434 - LOGID\_ATTCK\_ANOMALY\_OTHERS

**Message ID:** 18434

**Message Description:** LOGID\_ATTCK\_ANOMALY\_OTHERS

**Message Meaning:** Attack detected by other anomaly

**Type:** Anomaly

**Category:** ANOMALY

**Severity:** Alert

Log Field Name	Description	Data Type	Length
action	Action	string	16
attack	Attack	string	256
attackid	Attack ID	uint32	10
count	Count	uint32	10
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation Level	string	10

Log Field Name	Description	Data Type	Length
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log Message	string	518
policyid	Policy ID	uint32	10
policytype	Policy type	string	24
proto	Protocol	uint8	3
ref	Reference	string	4096
service	Name of Service	string	80
sessionid	Session ID	uint32	10
severity	Severity	string	8
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User	string	256
vd	Virtual Domain Name	string	32
vrf	Virtual router forwarding	uint8	3

## App

### 28672 - LOGID\_APP\_CTRL\_IM\_BASIC

**Message ID:** 28672

**Message Description:** LOGID\_APP\_CTRL\_IM\_BASIC

**Message Meaning:** Application control IM-basic

**Type:** App

**Category:** SIGNATURE

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64
applist	Application Control profile name	string	64
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Deivce ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64

Log Field Name	Description	Data Type	Length
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## 28673 - LOGID\_APP\_CTRL\_IM\_BASIC\_WITH\_STATUS

**Message ID:** 28673

**Message Description:** LOGID\_APP\_CTRL\_IM\_BASIC\_WITH\_STATUS

**Message Meaning:** Application control IM

**Type:** App

**Category:** SIGNATURE

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64
applist	Application Control profile name	string	64
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36



Log Field Name	Description	Data Type	Length
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## 28674 - LOGID\_APP\_CTRL\_IM\_BASIC\_WITH\_COUNT

**Message ID:** 28674

**Message Description:** LOGID\_APP\_CTRL\_IM\_BASIC\_WITH\_COUNT

**Message Meaning:** Application control IM (chat message count)

**Type:** App

**Category:** SIGNATURE

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16

Log Field Name	Description	Data Type	Length
app	Application name	string	96
appcat	Application category name	string	64
applist	Application Control profile name	string	64
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8

Log Field Name	Description	Data Type	Length
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## 28675 - LOGID\_APP\_CTRL\_IM\_FILE

**Message ID:** 28675

**Message Description:** LOGID\_APP\_CTRL\_IM\_FILE

**Message Meaning:** Application control IM (file)

**Type:** App

**Category:** SIGNATURE

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64
applist	Application Control profile name	string	64
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## 28676 - LOGID\_APP\_CTRL\_IM\_CHAT

**Message ID:** 28676

**Message Description:** LOGID\_APP\_CTRL\_IM\_CHAT

**Message Meaning:** Application control IM (chat)

**Type:** App

**Category:** SIGNATURE

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64
applist	Application Control profile name	string	64
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## 28677 - LOGID\_APP\_CTRL\_IM\_CHAT\_BLOCK

**Message ID:** 28677

**Message Description:** LOGID\_APP\_CTRL\_IM\_CHAT\_BLOCK

**Message Meaning:** Application control IM (chat blocked)

**Type:** App

**Category:** SIGNATURE

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64
applist	Application Control profile name	string	64

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66

Log Field Name	Description	Data Type	Length
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## 28678 - LOGID\_APP\_CTRL\_IM\_BLOCK

**Message ID:** 28678

**Message Description:** LOGID\_APP\_CTRL\_IM\_BLOCK

**Message Meaning:** Application control IM (blocked)

**Type:** App

**Category:** SIGNATURE

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64
applist	Application Control profile name	string	64
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32



Log Field Name	Description	Data Type	Length
fctuid	FortiClient User ID	string	32
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## 28704 - LOGID\_APP\_CTRL\_IPS\_PASS

**Message ID:** 28704

**Message Description:** LOGID\_APP\_CTRL\_IPS\_PASS

**Message Meaning:** Application control (IPS) (pass)

**Type:** App

**Category:** SIGNATURE

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64
applist	Application Control profile name	string	64
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10

Log Field Name	Description	Data Type	Length
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3
appid	Application ID	uint32	10
apprisk	Application risk level	string	16
ccertissuer		string	64
cloudaction	Action performed by cloud application	string	32
clouduser	User login ID detected by the Deep Application Control feature	string	256
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
filename	File name	string	256
filesize	File size in bytes	uint64	10
forwardedfor	Forwarded For	string	128
hostname	The host name of a URL	string	256
incidentserialno	Incident serial number	uint32	10
msg	Log message	string	512
parameters		string	512
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rawdataid		string	10
scertcname	server certificate name	string	64

Log Field Name	Description	Data Type	Length
scertissuer	server certificate issuer	string	64
trueclntip	True-Client-IP	ip	39
url	The URL address	string	512

## 28705 - LOGID\_APP\_CTRL\_IPS\_BLOCK

**Message ID:** 28705

**Message Description:** LOGID\_APP\_CTRL\_IPS\_BLOCK

**Message Meaning:** Application control (IPS) (block)

**Type:** App

**Category:** SIGNATURE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64
applist	Application Control profile name	string	64
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Deivce ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
ftuid	FortiClient User ID	string	32

Log Field Name	Description	Data Type	Length
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3
appid	Application ID	uint32	10
apprisk	Application risk level	string	16
ccertissuer		string	64
cloudaction	Action performed by cloud application	string	32
clouduser	User login ID detected by the Deep Application Control feature	string	256
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation Level	string	10

Log Field Name	Description	Data Type	Length
crscore	Client Reputation Score	uint32	10
filename	File name	string	256
filesize	File size in bytes	uint64	10
forwardedfor	Forwarded For	string	128
hostname	The host name of a URL	string	256
incidentserialno	Incident serial number	uint32	10
msg	Log message	string	512
parameters		string	512
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rawdataid		string	10
scertcname	server certificate name	string	64
scertissuer	server certificate issuer	string	64
trueclntip	True-Client-IP	ip	39
url	The URL address	string	512

## 28706 - LOGID\_APP\_CTRL\_IPS\_RESET

**Message ID:** 28706

**Message Description:** LOGID\_APP\_CTRL\_IPS\_RESET

**Message Meaning:** Application control (IPS) (reset)

**Type:** App

**Category:** SIGNATURE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64

Log Field Name	Description	Data Type	Length
applist	Application Control profile name	string	64
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz		string	5

Log Field Name	Description	Data Type	Length
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3
appid	Application ID	uint32	10
apprisk	Application risk level	string	16
ccertissuer		string	64
cloudaction	Action performed by cloud application	string	32
clouduser	User login ID detected by the Deep Application Control feature	string	256
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
filename	File name	string	256
filesize	File size in bytes	uint64	10
forwardedfor	Forwarded For	string	128
hostname	The host name of a URL	string	256
incidentserialno	Incident serial number	uint32	10
msg	Log message	string	512
parameters		string	512
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rawdataid		string	10
scertcname	server certificate name	string	64
scertissuer	server certificate issuer	string	64
trueclntip	True-Client-IP	ip	39
url	The URL address	string	512

## 28720 - LOGID\_APP\_CTRL\_SSH\_PASS

**Message ID:** 28720

**Message Description:** LOGID\_APP\_CTRL\_SSH\_PASS



**Message Meaning:** Application control IM (SSH) (pass)

**Type:** App

**Category:** SIGNATURE

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64
applist	Application Control profile name	string	64
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## 28721 - LOGID\_APP\_CTRL\_SSH\_BLOCK

**Message ID:** 28721

**Message Description:** LOGID\_APP\_CTRL\_SSH\_BLOCK

**Message Meaning:** Application control IM (SSH) (block)

**Type:** App

**Category:** SIGNATURE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64
applist	Application Control profile name	string	64

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
group	User group name	string	64
level	Log level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
service	Service name	string	80
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66

Log Field Name	Description	Data Type	Length
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## 28736 - LOGID\_APP\_CTRL\_PORT\_ENF

**Message ID:** 28736

**Message Description:** LOGID\_APP\_CTRL\_PORT\_ENF

**Message Meaning:** Application control port enforcement

**Type:** App

**Category:** PORT-VIOLATION

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96
appcat	Application category name	string	64
appid	Application ID	uint32	10
applist	Application Control profile name	string	64
apprisk	Application risk level	string	16
authserver	Authentication server for the user	string	64
ccertissuer		string	64
cloudaction	Action performed by cloud application	string	32
clouduser	User login ID detected by the Deep Application Control feature	string	256
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
filename	File name	string	256
filesize	File size in bytes	uint64	10
forwardedfor	Forwarded For	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
incidentserialno	Incident serial number	uint32	10
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	512
parameters		string	512
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rawdataid		string	10
scertcname	server certificate name	string	64
scertissuer	server certificate issuer	string	64
service	Service name	string	80
sessionid	Session ID	uint32	10

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP	ip	39
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## 28737 - LOGID\_APP\_CTRL\_PROTO\_ENF

**Message ID:** 28737

**Message Description:** LOGID\_APP\_CTRL\_PROTO\_ENF

**Message Meaning:** Application control protocol enforcement

**Type:** App

**Category:** PROTOCOL-VIOLATION

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: pass - Application is allowed block - Application is blocked (silent) reject - Quarantine reset - Application is blocked and Reset was sent Sometimes, there is a block page for blocking	string	16
app	Application name	string	96

Log Field Name	Description	Data Type	Length
appcat	Application category name	string	64
appid	Application ID	uint32	10
applist	Application Control profile name	string	64
apprisk	Application risk level	string	16
authserver	Authentication server for the user	string	64
ccertissuer		string	64
cloudaction	Action performed by cloud application	string	32
clouduser	User login ID detected by the Deep Application Control feature	string	256
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Time	uint64	20
eventtype	App Control Event Type	string	32
fctuid	FortiClient User ID	string	32
filename	File name	string	256
filesize	File size in bytes	uint64	10
forwardedfor	Forwarded For	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
incidentserialno	Incident serial number	uint32	10
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
parameters		string	512
policyid	Policy ID	uint32	10
profile		string	36
profiletype	Profile Type	string	36
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rawdataid		string	10
scertcname	server certificate name	string	64
scertissuer	server certificate issuer	string	64
service	Service name	string	80
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP	ip	39
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3



## AV

## 8192 - MESGID\_INFECT\_WARNING

**Message ID:** 8192**Message Description:** MESGID\_INFECT\_WARNING**Message Meaning:** Infected file detected by the FortiGate unit and blocked**Type:** AV**Category:** INFECTED**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39

Log Field Name	Description	Data Type	Length
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8193 - MESGID\_INFECT\_NOTIF

**Message ID:** 8193

**Message Description:** MESGID\_INFECT\_NOTIF

**Message Meaning:** Infected file detected by the FortiGate unit and it passed

**Type:** AV

**Category:** INFECTED

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128

Log Field Name	Description	Data Type	Length
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512

Log Field Name	Description	Data Type	Length
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8194 - MESGID\_INFECT\_MIME\_WARNING

**Message ID:** 8194

**Message Description:** MESGID\_INFECT\_MIME\_WARNING

**Message Meaning:** MIME header detected to have a virus and blocked

**Type:** AV

**Category:** INFECTED

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10

Log Field Name	Description	Data Type	Length
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5

Log Field Name	Description	Data Type	Length
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8195 - MESGID\_INFECT\_MIME\_NOTIF

**Message ID:** 8195

**Message Description:** MESGID\_INFECT\_MIME\_NOTIF

**Message Meaning:** MIME header infected and passed

**Type:** AV

**Category:** INFECTED

**Severity:** Notice



Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32

Log Field Name	Description	Data Type	Length
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16

Log Field Name	Description	Data Type	Length
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8200 - MESGID\_MIME\_FILETYPE\_EXE\_WARNING

**Message ID:** 8200

**Message Description:** MESGID\_MIME\_FILETYPE\_EXE\_WARNING

**Message Meaning:** File is an executable (warning)

**Type:** AV

**Category:** FILETYPE-EXECUTABLE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
checksum	The checksum of the scanned file	string	16
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10

Log Field Name	Description	Data Type	Length
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filename	File name	string	256
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39

Log Field Name	Description	Data Type	Length
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8201 - MESGID\_MIME\_FILETYPE\_EXE\_NOTIF

**Message ID:** 8201

**Message Description:** MESGID\_MIME\_FILETYPE\_EXE\_NOTIF

**Message Meaning:** File is an executable (notice)

**Type:** AV

**Category:** FILETYPE-EXECUTABLE

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3

Log Field Name	Description	Data Type	Length
authserver	Server used to authenticate the involved user	string	64
cc		string	512
checksum	The checksum of the scanned file	string	16
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filename	File name	string	256
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128

Log Field Name	Description	Data Type	Length
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8202 - MESGID\_AVQUERY\_WARNING

**Message ID:** 8202

**Message Description:** MESGID\_AVQUERY\_WARNING

**Message Meaning:** File reported infected by Outbreak Prevention (warning)

**Type:** AV

**Category:** OUTBREAK-PREVENTION

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32



Log Field Name	Description	Data Type	Length
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16

Log Field Name	Description	Data Type	Length
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8203 - MESGID\_AVQUERY\_NOTIF

**Message ID:** 8203

**Message Description:** MESGID\_AVQUERY\_NOTIF

**Message Meaning:** File reported infected by Outbreak Prevention (notice)

**Type:** AV

**Category:** OUTBREAK-PREVENTION

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13

Log Field Name	Description	Data Type	Length
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024

Log Field Name	Description	Data Type	Length
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8204 - MESGID\_MIME\_AVQUERY\_WARNING

**Message ID:** 8204

**Message Description:** MESGID\_MIME\_AVQUERY\_WARNING

**Message Meaning:** MIME data reported infected by Outbreak Prevention (warning)

**Type:** AV**Category:** OUTBREAK-PREVENTION**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64

Log Field Name	Description	Data Type	Length
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512

Log Field Name	Description	Data Type	Length
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8205 - MESGID\_MIME\_AVQUERY\_NOTIF

**Message ID:** 8205

**Message Description:** MESGID\_MIME\_AVQUERY\_NOTIF

**Message Meaning:** MIME data reported infected by Outbreak Prevention (notice)

**Type:** AV

**Category:** OUTBREAK-PREVENTION

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256

Log Field Name	Description	Data Type	Length
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3



Log Field Name	Description	Data Type	Length
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8212 - MESGID\_MALWARE\_LIST\_WARNING

**Message ID:** 8212

**Message Description:** MESGID\_MALWARE\_LIST\_WARNING

**Message Meaning:** File reported infected by external malware list (warning)

**Type:** AV

**Category:** MALWARE-LIST

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32

Log Field Name	Description	Data Type	Length
ftctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20

Log Field Name	Description	Data Type	Length
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8213 - MESGID\_MALWARE\_LIST\_NOTIF

**Message ID:** 8213

**Message Description:** MESGID\_MALWARE\_LIST\_NOTIF

**Message Meaning:** File reported infected by external malware list (notice)

**Type:** AV

**Category:** MALWARE-LIST

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3

Log Field Name	Description	Data Type	Length
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8214 - MESGID\_MIME\_MALWARE\_LIST\_WARNING

**Message ID:** 8214

**Message Description:** MESGID\_MIME\_MALWARE\_LIST\_WARNING

**Message Meaning:** MIME data reported infected by external malware list (warning)

**Type:** AV

**Category:** MALWARE-LIST

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32

Log Field Name	Description	Data Type	Length
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256



Log Field Name	Description	Data Type	Length
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8215 - MESGID\_MIME\_MALWARE\_LIST\_NOTIF

**Message ID:** 8215

**Message Description:** MESGID\_MIME\_MALWARE\_LIST\_NOTIF

**Message Meaning:** MIME data reported infected by external malware list (notice)

**Type:** AV

**Category:** MALWARE-LIST

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64

Log Field Name	Description	Data Type	Length
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32

Log Field Name	Description	Data Type	Length
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8448 - MESGID\_BLOCK\_WARNING

**Message ID:** 8448

**Message Description:** MESGID\_BLOCK\_WARNING

**Message Meaning:** FortiGate unit blocked a file because it contains a virus

**Type:** AV

**Category:** FILENAME

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
checksum	The checksum of the scanned file	string	16
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filefilter	The filter used to identify the affected file	string	12
filename	File name	string	256
filetype	File type	string	16
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16

Log Field Name	Description	Data Type	Length
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8450 - MESGID\_BLOCK\_MIME\_WARNING

**Message ID:** 8450

**Message Description:** MESGID\_BLOCK\_MIME\_WARNING

**Message Meaning:** FortiGate unit blocked a file because it contains a virus (MIME)

**Type:** AV

**Category:** MIMEFRAGMENTED

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
checksum	The checksum of the scanned file	string	16
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8

Log Field Name	Description	Data Type	Length
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filefilter	The filter used to identify the affected file	string	12
filename	File name	string	256
filetype	File type	string	16
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16

Log Field Name	Description	Data Type	Length
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8451 - MESGID\_BLOCK\_MIME\_NOTIF

**Message ID:** 8451

**Message Description:** MESGID\_BLOCK\_MIME\_NOTIF

**Message Meaning:** FortiGate unit blocked a file because it contains a virus (MIME)

**Type:** AV

**Category:** MIMEFRAGMENTED

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
checksum	The checksum of the scanned file	string	16
crackion	Threat Weight action	uint32	10



Log Field Name	Description	Data Type	Length
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filefilter	The filter used to identify the affected file	string	12
filename	File name	string	256
filetype	File type	string	16
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8452 - MESGID\_BLOCK\_COMMAND

**Message ID:** 8452

**Message Description:** MESGID\_BLOCK\_COMMAND

**Message Meaning:** FortiGate unit blocked a virus command

**Type:** AV

**Category:** COMMAND-BLOCKED

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64

Log Field Name	Description	Data Type	Length
authserver	Server used to authenticate the involved user	string	64
command		string	16
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subservice		string	16

Log Field Name	Description	Data Type	Length
subtype	Subtype of the virus log	string	20
time	Time	string	8
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8704 - MESGID\_OVERSIZE\_WARNING

**Message ID:** 8704

**Message Description:** MESGID\_OVERSIZE\_WARNING

**Message Meaning:** Defined file size limit was exceeded

**Type:** AV

**Category:** OVERSIZE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Server used to authenticate the involved user	string	64
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8

Log Field Name	Description	Data Type	Length
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filename	File name	string	256
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512

Log Field Name	Description	Data Type	Length
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8705 - MESGID\_OVERSIZE\_NOTIF

**Message ID:** 8705

**Message Description:** MESGID\_OVERSIZE\_NOTIF

**Message Meaning:** File size limit was exceeded

**Type:** AV

**Category:** OVERSIZE

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Server used to authenticate the involved user	string	64
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32

Log Field Name	Description	Data Type	Length
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filename	File name	string	256
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39

Log Field Name	Description	Data Type	Length
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8706 - MESGID\_OVERSIZE\_MIME\_WARNING

**Message ID:** 8706

**Message Description:** MESGID\_OVERSIZE\_MIME\_WARNING

**Message Meaning:** File (MIME) size exceed the defined size limit

**Type:** AV

**Category:** OVERSIZE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Server used to authenticate the involved user	string	64
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10



Log Field Name	Description	Data Type	Length
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filename	File name	string	256
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16

Log Field Name	Description	Data Type	Length
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8707 - MESGID\_OVERSIZE\_MIME\_NOTIF

**Message ID:** 8707

**Message Description:** MESGID\_OVERSIZE\_MIME\_NOTIF

**Message Meaning:** File (MIME) size exceed the defined size limit

**Type:** AV

**Category:** OVERSIZE

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Server used to authenticate the involved user	string	64
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
ftuid	Forticlient user ID	string	32
filename	File name	string	256
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5

Log Field Name	Description	Data Type	Length
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8708 - MESGID\_OVERSIZE\_STREAM\_UNCOMP\_WARNING

**Message ID:** 8708

**Message Description:** MESGID\_OVERSIZE\_STREAM\_UNCOMP\_WARNING

**Message Meaning:** Stream-based uncompression reached size limit.

**Type:** AV

**Category:** OVERSIZE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Server used to authenticate the involved user	string	64
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filename	File name	string	256
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66

Log Field Name	Description	Data Type	Length
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8709 - MESGID\_OVERSIZE\_STREAM\_UNCOMP\_NOTIF

**Message ID:** 8709

**Message Description:** MESGID\_OVERSIZE\_STREAM\_UNCOMP\_NOTIF

**Message Meaning:** Stream-based uncompression reached size limit.

**Type:** AV

**Category:** OVERSIZE

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Server used to authenticate the involved user	string	64
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20

Log Field Name	Description	Data Type	Length
eventtype	Event type of AV	string	32
ftuid	Forticlient user ID	string	32
filename	File name	string	256
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66

Log Field Name	Description	Data Type	Length
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8720 - MESGID\_SWITCH\_PROTO\_WARNING

**Message ID:** 8720

**Message Description:** MESGID\_SWITCH\_PROTO\_WARNING

**Message Meaning:** Switching protocols request (warning)

**Type:** AV

**Category:** SWITCHPROTO

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Server used to authenticate the involved user	string	64
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32



Log Field Name	Description	Data Type	Length
ftcluid	Forticlient user ID	string	32
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subservice		string	16
subtype	Subtype of the virus log	string	20
switchproto	Protocol used on the switch	string	128
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8721 - MESGID\_SWITCH\_PROTO\_NOTIF

**Message ID:** 8721

**Message Description:** MESGID\_SWITCH\_PROTO\_NOTIF

**Message Meaning:** Switching protocols request (notice)

**Type:** AV

**Category:** SWITCHPROTO

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Server used to authenticate the involved user	string	64
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subservice		string	16
subtype	Subtype of the virus log	string	20
switchproto	Protocol used on the switch	string	128
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## 8960 - MESGID\_SCAN\_UNCOMPSizeLIMIT\_WARNING

**Message ID:** 8960

**Message Description:** MESGID\_SCAN\_UNCOMPSizeLIMIT\_WARNING

**Message Meaning:** File reached the uncompressed nested limit

**Type:** AV

**Category:** SCANERROR

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32

Log Field Name	Description	Data Type	Length
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16

Log Field Name	Description	Data Type	Length
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8961 - MESGID\_SCAN\_UNCOMPSizeLIMIT\_NOTIF

**Message ID:** 8961

**Message Description:** MESGID\_SCAN\_UNCOMPSizeLIMIT\_NOTIF

**Message Meaning:** File reached the uncompressed size limit

**Type:** AV

**Category:** SCANERROR

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13

Log Field Name	Description	Data Type	Length
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024

Log Field Name	Description	Data Type	Length
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8962 - MESGID\_SCAN\_ARCHIVE\_ENCRYPTED\_WARNING

**Message ID:** 8962

**Message Description:** MESGID\_SCAN\_ARCHIVE\_ENCRYPTED\_WARNING

**Message Meaning:** Archived file is corrupted



**Type:** AV**Category:** SCANERROR**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64

Log Field Name	Description	Data Type	Length
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512

Log Field Name	Description	Data Type	Length
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8963 - MESGID\_SCAN\_ARCHIVE\_ENCRYPTED\_NOTIF

**Message ID:** 8963

**Message Description:** MESGID\_SCAN\_ARCHIVE\_ENCRYPTED\_NOTIF

**Message Meaning:** Archived file is encrypted

**Type:** AV

**Category:** SCANERROR

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256

Log Field Name	Description	Data Type	Length
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8964 - MESGID\_SCAN\_ARCHIVE\_CORRUPTED\_WARNING

**Message ID:** 8964

**Message Description:** MESGID\_SCAN\_ARCHIVE\_CORRUPTED\_WARNING

**Message Meaning:** Corrupted archive (warning)

**Type:** AV

**Category:** SCANERROR

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32

Log Field Name	Description	Data Type	Length
ftctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20

Log Field Name	Description	Data Type	Length
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8965 - MESGID\_SCAN\_ARCHIVE\_CORRUPTED\_NOTIF

**Message ID:** 8965

**Message Description:** MESGID\_SCAN\_ARCHIVE\_CORRUPTED\_NOTIF

**Message Meaning:** Corrupted archive (notice)

**Type:** AV

**Category:** SCANERROR

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3



Log Field Name	Description	Data Type	Length
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8966 - MESGID\_SCAN\_ARCHIVE\_MULTIPART\_WARNING

**Message ID:** 8966

**Message Description:** MESGID\_SCAN\_ARCHIVE\_MULTIPART\_WARNING

**Message Meaning:** File is a multipart archive or contains multiple files within the archive

**Type:** AV

**Category:** SCANERROR

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32

Log Field Name	Description	Data Type	Length
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256

Log Field Name	Description	Data Type	Length
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8967 - MESGID\_SCAN\_ARCHIVE\_MULTIPART\_NOTIF

**Message ID:** 8967

**Message Description:** MESGID\_SCAN\_ARCHIVE\_MULTIPART\_NOTIF

**Message Meaning:** File is a multipart archive or contains multiple files within the archive

**Type:** AV

**Category:** SCANERROR

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64

Log Field Name	Description	Data Type	Length
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32

Log Field Name	Description	Data Type	Length
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8968 - MESGID\_SCAN\_ARCHIVE\_NESTED\_WARNING

**Message ID:** 8968

**Message Description:** MESGID\_SCAN\_ARCHIVE\_NESTED\_WARNING

**Message Meaning:** File is a nested archived file

**Type:** AV

**Category:** SCANERROR

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8



Log Field Name	Description	Data Type	Length
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8969 - MESGID\_SCAN\_ARCHIVE\_NESTED\_NOTIF

**Message ID:** 8969

**Message Description:** MESGID\_SCAN\_ARCHIVE\_NESTED\_NOTIF

**Message Meaning:** File is an archived type unhandled

**Type:** AV

**Category:** SCANERROR

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32

Log Field Name	Description	Data Type	Length
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16

Log Field Name	Description	Data Type	Length
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8970 - MESGID\_SCAN\_ARCHIVE\_OVERSIZE\_WARNING

**Message ID:** 8970

**Message Description:** MESGID\_SCAN\_ARCHIVE\_OVERSIZE\_WARNING

**Message Meaning:** Archived file is oversized

**Type:** AV

**Category:** SCANERROR

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13

Log Field Name	Description	Data Type	Length
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024

Log Field Name	Description	Data Type	Length
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8971 - MESGID\_SCAN\_ARCHIVE\_OVERSIZE\_NOTIF

**Message ID:** 8971

**Message Description:** MESGID\_SCAN\_ARCHIVE\_OVERSIZE\_NOTIF

**Message Meaning:** Archived file is oversized

**Type:** AV**Category:** SCANERROR**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64



Log Field Name	Description	Data Type	Length
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512

Log Field Name	Description	Data Type	Length
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8972 - MESGID\_SCAN\_ARCHIVE\_UNHANDLED\_WARNING

**Message ID:** 8972

**Message Description:** MESGID\_SCAN\_ARCHIVE\_UNHANDLED\_WARNING

**Message Meaning:** Unhandled archive (warning)

**Type:** AV

**Category:** SCANERROR

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256

Log Field Name	Description	Data Type	Length
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8973 - MESGID\_SCAN\_ARCHIVE\_UNHANDLED\_NOTIF

**Message ID:** 8973

**Message Description:** MESGID\_SCAN\_ARCHIVE\_UNHANDLED\_NOTIF

**Message Meaning:** Unhandled archive (notice)

**Type:** AV

**Category:** SCANERROR

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32

Log Field Name	Description	Data Type	Length
ftctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20

Log Field Name	Description	Data Type	Length
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8974 - MESGID\_SCAN\_AV\_ENGINE\_LOAD\_FAILED\_ERROR

**Message ID:** 8974

**Message Description:** MESGID\_SCAN\_AV\_ENGINE\_LOAD\_FAILED\_ERROR

**Message Meaning:** AV Engine load failed

**Type:** AV

**Category:** SCANERROR

**Severity:** Error

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3

Log Field Name	Description	Data Type	Length
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096



Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8975 - MESGID\_SCAN\_ARCHIVE\_PARTIALLYCORRUPTED\_WARNING

**Message ID:** 8975

**Message Description:** MESGID\_SCAN\_ARCHIVE\_PARTIALLYCORRUPTED\_WARNING

**Message Meaning:** Partially corrupted archive (warning)

**Type:** AV

**Category:** SCANERROR

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32

Log Field Name	Description	Data Type	Length
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256

Log Field Name	Description	Data Type	Length
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8976 - MESGID\_SCAN\_ARCHIVE\_PARTIALLYCORRUPTED\_NOTIF

**Message ID:** 8976

**Message Description:** MESGID\_SCAN\_ARCHIVE\_PARTIALLYCORRUPTED\_NOTIF

**Message Meaning:** Partially corrupted archive (notice)

**Type:** AV

**Category:** SCANERROR

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64

Log Field Name	Description	Data Type	Length
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32

Log Field Name	Description	Data Type	Length
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8977 - MESGID\_SCAN\_ARCHIVE\_FILESLIMIT\_WARNING

**Message ID:** 8977

**Message Description:** MESGID\_SCAN\_ARCHIVE\_FILESLIMIT\_WARNING

**Message Meaning:** Exceeded archive files limit (warning)

**Type:** AV

**Category:** SCANERROR

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8

Log Field Name	Description	Data Type	Length
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255



Log Field Name	Description	Data Type	Length
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8978 - MESGID\_SCAN\_ARCHIVE\_FILESLIMIT\_NOTIF

**Message ID:** 8978

**Message Description:** MESGID\_SCAN\_ARCHIVE\_FILESLIMIT\_NOTIF

**Message Meaning:** Exceeded archive files limit (notice)

**Type:** AV

**Category:** SCANERROR

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32

Log Field Name	Description	Data Type	Length
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16

Log Field Name	Description	Data Type	Length
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8979 - MESGID\_SCAN\_ARCHIVE\_TIMEOUT\_WARNING

**Message ID:** 8979

**Message Description:** MESGID\_SCAN\_ARCHIVE\_TIMEOUT\_WARNING

**Message Meaning:** Archive scan timeout (warning)

**Type:** AV

**Category:** SCANERROR

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13

Log Field Name	Description	Data Type	Length
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024

Log Field Name	Description	Data Type	Length
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8980 - MESGID\_SCAN\_ARCHIVE\_TIMEOUT\_NOTIF

**Message ID:** 8980

**Message Description:** MESGID\_SCAN\_ARCHIVE\_TIMEOUT\_NOTIF

**Message Meaning:** Archive scan timeout (notice)

**Type:** AV**Category:** SCANERROR**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64

Log Field Name	Description	Data Type	Length
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512



Log Field Name	Description	Data Type	Length
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 8981 - MESGID\_SCAN\_AV\_CDR\_INTERNAL\_ERROR

**Message ID:** 8981

**Message Description:** MESGID\_SCAN\_AV\_CDR\_INTERNAL\_ERROR

**Message Meaning:** AV CDR engine internal error

**Type:** AV

**Category:** SCANERROR

**Severity:** Error

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256

Log Field Name	Description	Data Type	Length
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 9233 - MESGID\_ANALYTICS\_SUBMITTED

**Message ID:** 9233

**Message Description:** MESGID\_ANALYTICS\_SUBMITTED**Message Meaning:** File submitted to Sandbox**Type:** AV**Category:** ANALYTICS**Severity:** Information

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32

Log Field Name	Description	Data Type	Length
ftctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20

Log Field Name	Description	Data Type	Length
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 9234 - MESGID\_ANALYTICS\_INFECT\_WARNING

**Message ID:** 9234

**Message Description:** MESGID\_ANALYTICS\_INFECT\_WARNING

**Message Meaning:** File reported infected by FortiSandbox (warning)

**Type:** AV

**Category:** INFECTED

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3

Log Field Name	Description	Data Type	Length
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3



## 9235 - MESGID\_ANALYTICS\_INFECT\_NOTIF

**Message ID:** 9235

**Message Description:** MESGID\_ANALYTICS\_INFECT\_NOTIF

**Message Meaning:** File reported infected by FortiSandbox (notice)

**Type:** AV

**Category:** INFECTED

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32

Log Field Name	Description	Data Type	Length
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256

Log Field Name	Description	Data Type	Length
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 9236 - MESGID\_ANALYTICS\_INFECT\_MIME\_WARNING

**Message ID:** 9236

**Message Description:** MESGID\_ANALYTICS\_INFECT\_MIME\_WARNING

**Message Meaning:** File reported infected by FortiSandbox (warning)

**Type:** AV

**Category:** INFECTED

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64

Log Field Name	Description	Data Type	Length
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32

Log Field Name	Description	Data Type	Length
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 9237 - MESGID\_ANALYTICS\_INFECT\_MIME\_NOTIF

**Message ID:** 9237

**Message Description:** MESGID\_ANALYTICS\_INFECT\_MIME\_NOTIF

**Message Meaning:** File reported infected by FortiSandbox (notice)

**Type:** AV

**Category:** INFECTED

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
agent	User agent - eg. agent="Mozilla/5.0"	string	64
analyticscksum	The checksum of the file submitted for analytics	string	64
analyticssubmit	The flag for analytics submission	string	10
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8

Log Field Name	Description	Data Type	Length
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filehash	Used by Outbreak Prevention External Hash: the hash signature used in the detection	string	64
filehashsrc	Used by Outbreak Prevention External Hash: external source that provided the hash signature	string	32
filename	File name	string	256
filetype	File type	string	16
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
quarskip	Quarantine skip explanation	string	46
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
ref	The URL of the FortiGuard IPS database entry for the attack	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
virus	Virus Name	string	128
virusid	Virus ID (unique virus identifier)	uint32	10
vrf		uint8	3

## 9238 - MESGID\_ANALYTICS\_FSA\_RESULT

**Message ID:** 9238

**Message Description:** MESGID\_ANALYTICS\_FSA\_RESULT

**Message Meaning:** File verdict returned from FortiSandbox

**Type:** AV

**Category:** ANALYTICS

**Severity:** Notice



Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
analyticscksum	The checksum of the file submitted for analytics	string	64
date	Date	string	10
devid		string	16
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
dtype	Data type for virus category	string	32
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filename	File name	string	256
level	Log level	string	11
logid	Log ID	string	10
service	Proxy service which scanned this traffic	string	5
srcdomain		string	255
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Subtype of the virus log	string	20
time	Time	string	8
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
vd	VDOM name	string	32
fsaverdict	FortiSandbox Verdict returned to FortiGate after analysis (clean, low risk, med risk, high risk, malicious)	string	32

## 9239 - MESGID\_CONTENT\_DISARM\_NOTIF

**Message ID:** 9239

**Message Description:** MESGID\_CONTENT\_DISARM\_NOTIF

**Message Meaning:** Active content detected by Content Disarm engine

**Type:** AV

**Category:** CONTENT-DISARM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
analyticscksum	The checksum of the file submitted for analytics	string	64
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filename	File name	string	256
forwardedfor		string	128

Log Field Name	Description	Data Type	Length
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256

Log Field Name	Description	Data Type	Length
vd	VDOM name	string	32
vrf		uint8	3

## 9240 - MESGID\_CONTENT\_DISARM\_WARNING

**Message ID:** 9240

**Message Description:** MESGID\_CONTENT\_DISARM\_WARNING

**Message Meaning:** File was disarmed by Content Disarm engine

**Type:** AV

**Category:** CONTENT-DISARM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	17
analyticscksum	The checksum of the file submitted for analytics	string	64
attachment		string	3
authserver	Server used to authenticate the involved user	string	64
cc		string	512
cdrcontent		string	256
checksum	The checksum of the scanned file	string	16
contentdisarmed	Content Disarm action- eg. disarmed, detected	string	13
craction	Threat Weight action	uint32	10
crlevel	Threat Weight Level	string	10
crscore	Threat Weight Score	uint32	10
date	Date	string	10
devid		string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	Event type of AV	string	32
fctuid	Forticlient user ID	string	32
filename	File name	string	256
forwardedfor		string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	Group name (authentication)	string	64
level	Log level	string	11
logid	Log ID	string	10
msg	Log message	string	4096
policyid	Policy ID	uint32	10
profile	The name of the profile that was used to detect and take action	string	64
proto	Protocol number	uint8	3
rawdata		string	1024
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Proxy service which scanned this traffic	string	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subject		string	256
subservice		string	16
subtype	Subtype of the virus log	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip		ip	39

Log Field Name	Description	Data Type	Length
type	Log type	string	16
tz	Time Zone	string	5
unauthuser		string	66
unauthusersource		string	66
url	The URL address	string	512
user	Username (authentication)	string	256
vd	VDOM name	string	32
vrf		uint8	3

## CIFS

### 63000 - LOG\_ID\_CIFS\_FILE\_BLOCK

**Message ID:** 63000

**Message Description:** LOG\_ID\_CIFS\_FILE\_BLOCK

**Message Meaning:** File was blocked by file filter

**Type:** CIFS

**Category:** CIFS-FILEFILTER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date		string	10
devid		string	16
domainctrlauthstate		uint32	5
domainctrlauthtype		uint32	5
domainctrldomain		string	80
domainctrlip		ip	39
domainctrlname		string	64
domainctrlprotocoltype		uint32	5
domainctrlusername		string	65
dstintf		string	32
dstintfrole		string	10

Log Field Name	Description	Data Type	Length
dstip		ip	39
dstport		uint16	5
errorcode		string	20
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
level		string	11
logid		string	10
msg		string	4096
policyid		uint32	10
profile		string	64
service		string	5
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
vd		string	32

## 63001 - LOG\_ID\_CIFS\_FILE\_PASS

**Message ID:** 63001

**Message Description:** LOG\_ID\_CIFS\_FILE\_PASS

**Message Meaning:** File detected by file-type filter

**Type:** CIFS

**Category:** CIFS-FILEFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date		string	10
devid		string	16
domainctrlauthstate		uint32	5
domainctrlauthtype		uint32	5
domainctrldomain		string	80
domainctrlip		ip	39
domainctrlname		string	64
domainctrlprotocoltype		uint32	5
domainctrlusername		string	65
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
errorcode		string	20
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
level		string	11
logid		string	10
msg		string	4096
policyid		uint32	10
profile		string	64
service		string	5
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8



Log Field Name	Description	Data Type	Length
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
vd		string	32

## 63002 - LOG\_ID\_CIFS\_CONN\_FAIL

**Message ID:** 63002

**Message Description:** LOG\_ID\_CIFS\_CONN\_FAIL

**Message Meaning:** Unable to connect to the CIFS Domain Controller

**Type:** CIFS

**Category:** CIFS-AUTH-FAIL

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date		string	10
devid		string	16
domainctrlauthstate		uint32	5
domainctrlauthtype		uint32	5
domainctrldomain		string	80
domainctrlip		ip	39
domainctrlname		string	64
domainctrlprotocoltype		uint32	5
domainctrlusername		string	65
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
errorcode		string	20
eventtime		uint64	20
eventtype		string	32

Log Field Name	Description	Data Type	Length
fctuid		string	32
level		string	11
logid		string	10
msg		string	4096
policyid		uint32	10
profile		string	64
service		string	5
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
vd		string	32

## 63003 - LOG\_ID\_CIFS\_AUTH\_FAIL

**Message ID:** 63003

**Message Description:** LOG\_ID\_CIFS\_AUTH\_FAIL

**Message Meaning:** Unable to authenticate with the CIFS Domain Controller

**Type:** CIFS

**Category:** CIFS-AUTH-FAIL

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date		string	10
devid		string	16

Log Field Name	Description	Data Type	Length
domainctrlauthstate		uint32	5
domainctrlauthtype		uint32	5
domainctrldomain		string	80
domainctrlip		ip	39
domainctrlname		string	64
domainctrlprotocoltype		uint32	5
domainctrlusername		string	65
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
errorcode		string	20
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
level		string	11
logid		string	10
msg		string	4096
policyid		uint32	10
profile		string	64
service		string	5
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5

Log Field Name	Description	Data Type	Length
unauthuser		string	66
unauthusersource		string	66
vd		string	32

## 63004 - LOG\_ID\_CIFS\_AUTH\_INTERNAL\_ERROR

**Message ID:** 63004

**Message Description:** LOG\_ID\_CIFS\_AUTH\_INTERNAL\_ERROR

**Message Meaning:** An error occurred in processing CIFS authentication

**Type:** CIFS

**Category:** CIFS-AUTH-FAIL

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date		string	10
devid		string	16
domainctrlauthstate		uint32	5
domainctrlauthtype		uint32	5
domainctrldomain		string	80
domainctrlip		ip	39
domainctrlname		string	64
domainctrlprotocoltype		uint32	5
domainctrlusername		string	65
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
errorcode		string	20
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
level		string	11

Log Field Name	Description	Data Type	Length
logid		string	10
msg		string	4096
policyid		uint32	10
profile		string	64
service		string	5
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
vd		string	32

## 63005 - LOG\_ID\_CIFS\_AUTH\_KRB\_ERROR

**Message ID:** 63005

**Message Description:** LOG\_ID\_CIFS\_AUTH\_KRB\_ERROR

**Message Meaning:** An error occurred in processing CIFS authentication.

**Type:** CIFS

**Category:** CIFS-AUTH-FAIL

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date		string	10
devid		string	16
domainctrlauthstate		uint32	5
domainctrlauthtype		uint32	5

Log Field Name	Description	Data Type	Length
domainctrldomain		string	80
domainctrlip		ip	39
domainctrlname		string	64
domainctrlprotocoltype		uint32	5
domainctrlusername		string	65
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
errorcode		string	20
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
level		string	11
logid		string	10
msg		string	4096
policyid		uint32	10
profile		string	64
service		string	5
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
vd		string	32

## DLP

### 24576 - LOG\_ID\_DLP\_WARN

**Message ID:** 24576

**Message Description:** LOG\_ID\_DLP\_WARN

**Message Meaning:** Data leak detected by specified DLP sensor rule

**Type:** DLP

**Category:** DLP

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: log-only - DLP event is detected , but NOT blocked (similar to monitor action) block - Blocked exempt - Allowed ban - blocked (Not in used since FortiOS 5.0, replaced by blocked) ban-sender - blocks all data being sent by an ip or user (Not in used since FortiOS 5.0, replaced by quarantine) quarantine-ip - Blocked and band the source ip (Not in used since FortiOS 5.0) quarantine-interface - Blocked and band the source interface (Not in used since FortiOS 5.0)	string	20
agent	User agent - eg. agent="Mozilla/5.0"	string	64
attachment		string	3
authserver	Authentication Server	string	64
cc		string	512
date	Date	string	10
devid	Device ID	string	16
direction	Direction of packets	string	8
dlpextra	DLP extra information	string	256
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
epoch	Epoch used for locating file	uint32	10
eventid	The serial number of the dlparchive file in the same epoch	uint32	10
eventtime	Event Time, time when DLP event detected.	uint64	20
eventtype	DLP event type	string	32
fctuid	FortiClient User ID	string	32
filename	File name	string	256
filesize	File size in bytes	uint64	10
filetype	File type	string	23
filtercat	DLP filter category	string	8
filteridx	DLP filter ID	uint32	10
filtername	DLP rule name	string	128
filtertype	DLP filter type	string	23
forwardedfor	Forwarded For	string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
infectedfilelevel	Infected File Level (Critical,Warning etc)	uint32	10
infectedfilename	Infected File Name	string	256
infectedfilesize	Infected File Size	uint64	10
infectedfiletype	Infected File Type	string	23
level	Log Level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile	DLP profile name	string	64
proto	Protocol number	uint8	3
rawdata	Raw Data	string	1024
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Service name	string	36
sessionid	Session ID	uint32	10



Log Field Name	Description	Data Type	Length
severity	Severity level of a DLP rule	string	8
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subject	The subject title of the email message	string	256
subservice		string	16
subtype	Log subtype	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip	True client's IP	ip	39
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## 24577 - LOG\_ID\_DLP\_NOTIF

**Message ID:** 24577

**Message Description:** LOG\_ID\_DLP\_NOTIF

**Message Meaning:** Data leak detected by specified DLP sensor rule

**Type:** DLP

**Category:** DLP

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: log-only - DLP event is detected , but NOT blocked (similar to monitor action) block - Blocked exempt - Allowed ban - blocked (Not in used since FortiOS 5.0, replaced by blocked) ban-sender - blocks all data being sent by an ip or user (Not in used since FortiOS 5.0, replaced by quarantine) quarantine-ip - Blocked and band the source ip (Not in used since FortiOS 5.0) quarantine-interface - Blocked and band the source interface (Not in used since FortiOS 5.0)	string	20
agent	User agent - eg. agent="Mozilla/5.0"	string	64
attachment		string	3
authserver	Authentication Server	string	64
cc		string	512
date	Date	string	10
devid	Device ID	string	16
direction	Direction of packets	string	8
dlpextra	DLP extra information	string	256
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
epoch	Epoch used for locating file	uint32	10
eventid	The serial number of the dlparchive file in the same epoch	uint32	10
eventtime	Event Time, time when DLP event detected.	uint64	20
eventtype	DLP event type	string	32
fctuid	FortiClient User ID	string	32
filename	File name	string	256
filesize	File size in bytes	uint64	10
filetype	File type	string	23
filtercat	DLP filter category	string	8

Log Field Name	Description	Data Type	Length
filteridx	DLP filter ID	uint32	10
filtername	DLP rule name	string	128
filtertype	DLP filter type	string	23
forwardedfor	Forwarded For	string	128
from	Email address from the Email Headers (IMAP/POP3/SMTP)	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
infectedfilelevel	Infected File Level (Critical,Warning etc)	uint32	10
infectedfilename	Infected File Name	string	256
infectedfilesize	Infected File Size	uint64	10
infectedfiletype	Infected File Type	string	23
level	Log Level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile	DLP profile name	string	64
proto	Protocol number	uint8	3
rawdata	Raw Data	string	1024
recipient	Email addresses from the SMTP envelope	string	512
sender	Email address from the SMTP envelope	string	128
service	Service name	string	36
sessionid	Session ID	uint32	10
severity	Severity level of a DLP rule	string	8
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subject	The subject title of the email message	string	256
subservice		string	16
subtype	Log subtype	string	20

Log Field Name	Description	Data Type	Length
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
trueclntip	True client's IP	ip	39
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual Routing Forwarding	uint8	3

## DNS

### 54000 - LOG\_ID\_DNS\_QUERY

**Message ID:** 54000

**Message Description:** LOG\_ID\_DNS\_QUERY

**Message Meaning:** DNS query message

**Type:** DNS

**Category:** DNS-QUERY

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
devid	Device ID	string	16
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface Role	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event Timestamp	uint64	20

Log Field Name	Description	Data Type	Length
eventtype	DNS Type (DNS query/DNS response)	string	32
fctuid	FortiClient ID	string	32
group	User group name	string	64
level	Log Level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile	Profile name for DNS filter	string	64
proto	Protocol number	uint8	3
qclass	Query class	string	32
qname	Query domain name	string	256
qtype	Query type description	string	32
qtypeval	Query Type Value	uint16	5
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface Role	string	10
srcip	Source IP	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name	string	256
vd	Virtual Domain Name	string	32
xid	Transaction ID	uint16	5

## 54200 - LOG\_ID\_DNS\_RESOLV\_ERROR

**Message ID:** 54200

**Message Description:** LOG\_ID\_DNS\_RESOLV\_ERROR**Message Meaning:** DNS resolution error message**Type:** DNS**Category:** DNS-RESPONSE**Severity:** Error

Log Field Name	Description	Data Type	Length
action	Security action performed by DNS filter	string	16
botnetdomain	Botnet domain name	string	256
botnetip	Botnet IP address	ip	39
cat	DNS category ID	uint8	3
catdesc	DNS category description	string	64
date	Date	string	10
devid	Device ID	string	16
domainfilteridx	Domain Filter Index	uint8	3
domainfilterlist	Domain Filter List	string	512
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface Role	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	DNS filter service error message	string	256
eventtime	Event Timestamp	uint64	20
eventtype	DNS Type (DNS query/DNS response)	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
fctuid	FortiClient ID	string	32
group	User group name	string	64
ipaddr	IP addresses from DNS response answer section	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Profile name for DNS filter	string	64
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
qclass	Query class	string	32
qname	Query domain name	string	256
qtype	Query type description	string	32
qtypeval	Query Type Value	uint16	5
rcode		uint8	3
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface Role	string	10
srcip	Source IP	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcport	Source Port	uint16	5
sscname	Safe Search CNAME	string	256
subtype	Log Subtype	string	20
time	Time	string	8
translationid		uint32	10
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name	string	256
vd	Virtual Domain Name	string	32
xid	Transaction ID	uint16	5

## 54400 - LOG\_ID\_DNS\_URL\_FILTER\_BLOCK

**Message ID:** 54400

**Message Description:** LOG\_ID\_DNS\_URL\_FILTER\_BLOCK

**Message Meaning:** Domain blocked because it is in the domain-filter list

**Type:** DNS

**Category:** DNS-RESPONSE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by DNS filter	string	16
botnetdomain	Botnet domain name	string	256
botnetip	Botnet IP address	ip	39
cat	DNS category ID	uint8	3
catdesc	DNS category description	string	64
date	Date	string	10
devid	Device ID	string	16
domainfilteridx	Domain Filter Index	uint8	3
domainfilterlist	Domain Filter List	string	512
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface Role	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	DNS filter service error message	string	256
eventtime	Event Timestamp	uint64	20
eventtype	DNS Type (DNS query/DNS response)	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
fctuid	FortiClient ID	string	32
group	User group name	string	64
ipaddr	IP addresses from DNS response answer section	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Profile name for DNS filter	string	64
proto	Protocol number	uint8	3
qclass	Query class	string	32
qname	Query domain name	string	256
qtype	Query type description	string	32
qtypeval	Query Type Value	uint16	5



Log Field Name	Description	Data Type	Length
rcode		uint8	3
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface Role	string	10
srcip	Source IP	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcport	Source Port	uint16	5
sscname	Safe Search CNAME	string	256
subtype	Log Subtype	string	20
time	Time	string	8
translationid		uint32	10
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name	string	256
vd	Virtual Domain Name	string	32
xid	Transaction ID	uint16	5

## 54401 - LOG\_ID\_DNS\_URL\_FILTER\_ALLOW

**Message ID:** 54401

**Message Description:** LOG\_ID\_DNS\_URL\_FILTER\_ALLOW

**Message Meaning:** Domain allowed because it is in the domain-filter list

**Type:** DNS

**Category:** DNS-RESPONSE

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action performed by DNS filter	string	16
botnetdomain	Botnet domain name	string	256

Log Field Name	Description	Data Type	Length
botnetip	Botnet IP address	ip	39
cat	DNS category ID	uint8	3
catdesc	DNS category description	string	64
date	Date	string	10
devid	Device ID	string	16
domainfilteridx	Domain Filter Index	uint8	3
domainfilterlist	Domain Filter List	string	512
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface Role	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	DNS filter service error message	string	256
eventtime	Event Timestamp	uint64	20
eventtype	DNS Type (DNS query/DNS response)	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
fctuid	FortiClient ID	string	32
group	User group name	string	64
ipaddr	IP addresses from DNS response answer section	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Profile name for DNS filter	string	64
proto	Protocol number	uint8	3
qclass	Query class	string	32
qname	Query domain name	string	256
qtype	Query type description	string	32
qtypeval	Query Type Value	uint16	5
rcode		uint8	3
sessionid	Session ID	uint32	10

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface Role	string	10
srcip	Source IP	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcport	Source Port	uint16	5
sscname	Safe Search CNAME	string	256
subtype	Log Subtype	string	20
time	Time	string	8
translationid		uint32	10
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name	string	256
vd	Virtual Domain Name	string	32
xid	Transaction ID	uint16	5

## 54600 - LOG\_ID\_DNS\_BOTNET\_IP

**Message ID:** 54600

**Message Description:** LOG\_ID\_DNS\_BOTNET\_IP

**Message Meaning:** Domain blocked by DNS botnet C&C (IP)

**Type:** DNS

**Category:** DNS-RESPONSE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by DNS filter	string	16
botnetdomain	Botnet domain name	string	256
botnetip	Botnet IP address	ip	39
cat	DNS category ID	uint8	3

Log Field Name	Description	Data Type	Length
catdesc	DNS category description	string	64
date	Date	string	10
devid	Device ID	string	16
domainfilteridx	Domain Filter Index	uint8	3
domainfilterlist	Domain Filter List	string	512
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface Role	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	DNS filter service error message	string	256
eventtime	Event Timestamp	uint64	20
eventtype	DNS Type (DNS query/DNS response)	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
fctuid	FortiClient ID	string	32
group	User group name	string	64
ipaddr	IP addresses from DNS response answer section	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Profile name for DNS filter	string	64
proto	Protocol number	uint8	3
qclass	Query class	string	32
qname	Query domain name	string	256
qtype	Query type description	string	32
qtypeval	Query Type Value	uint16	5
rcode		uint8	3
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32

Log Field Name	Description	Data Type	Length
srcintfrole	Source Interface Role	string	10
srcip	Source IP	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcport	Source Port	uint16	5
sscname	Safe Search CNAME	string	256
subtype	Log Subtype	string	20
time	Time	string	8
translationid		uint32	10
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name	string	256
vd	Virtual Domain Name	string	32
xid	Transaction ID	uint16	5

## 54601 - LOG\_ID\_DNS\_BOTNET\_DOMAIN

**Message ID:** 54601

**Message Description:** LOG\_ID\_DNS\_BOTNET\_DOMAIN

**Message Meaning:** Domain blocked by DNS botnet C&C (Domain)

**Type:** DNS

**Category:** DNS-RESPONSE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by DNS filter	string	16
botnetdomain	Botnet domain name	string	256
botnetip	Botnet IP address	ip	39
cat	DNS category ID	uint8	3
catdesc	DNS category description	string	64
date	Date	string	10

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
domainfilteridx	Domain Filter Index	uint8	3
domainfilterlist	Domain Filter List	string	512
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface Role	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	DNS filter service error message	string	256
eventtime	Event Timestamp	uint64	20
eventtype	DNS Type (DNS query/DNS response)	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
fctuid	FortiClient ID	string	32
group	User group name	string	64
ipaddr	IP addresses from DNS response answer section	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Profile name for DNS filter	string	64
proto	Protocol number	uint8	3
qclass	Query class	string	32
qname	Query domain name	string	256
qtype	Query type description	string	32
qtypeval	Query Type Value	uint16	5
rcode		uint8	3
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface Role	string	10
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
srcmac	MAC address associated with the Source IP	string	17
srcport	Source Port	uint16	5
sscname	Safe Search CNAME	string	256
subtype	Log Subtype	string	20
time	Time	string	8
translationid		uint32	10
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name	string	256
vd	Virtual Domain Name	string	32
xid	Transaction ID	uint16	5

## 54800 - LOG\_ID\_DNS\_FTGD\_WARNING

**Message ID:** 54800

**Message Description:** LOG\_ID\_DNS\_FTGD\_WARNING

**Message Meaning:** FortiGuard rating error warning

**Type:** DNS

**Category:** DNS-RESPONSE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by DNS filter	string	16
botnetdomain	Botnet domain name	string	256
botnetip	Botnet IP address	ip	39
cat	DNS category ID	uint8	3
catdesc	DNS category description	string	64
date	Date	string	10
devid	Device ID	string	16
domainfilteridx	Domain Filter Index	uint8	3

Log Field Name	Description	Data Type	Length
domainfilterlist	Domain Filter List	string	512
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface Role	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	DNS filter service error message	string	256
eventtime	Event Timestamp	uint64	20
eventtype	DNS Type (DNS query/DNS response)	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
fctuid	FortiClient ID	string	32
group	User group name	string	64
ipaddr	IP addresses from DNS response answer section	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Profile name for DNS filter	string	64
proto	Protocol number	uint8	3
qclass	Query class	string	32
qname	Query domain name	string	256
qtype	Query type description	string	32
qtypeval	Query Type Value	uint16	5
rcode		uint8	3
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface Role	string	10
srcip	Source IP	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcport	Source Port	uint16	5



Log Field Name	Description	Data Type	Length
sscname	Safe Search CNAME	string	256
subtype	Log Subtype	string	20
time	Time	string	8
translationid		uint32	10
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name	string	256
vd	Virtual Domain Name	string	32
xid	Transaction ID	uint16	5

## 54801 - LOG\_ID\_DNS\_FTGD\_ERROR

**Message ID:** 54801

**Message Description:** LOG\_ID\_DNS\_FTGD\_ERROR

**Message Meaning:** FortiGuard rating error occurred

**Type:** DNS

**Category:** DNS-RESPONSE

**Severity:** Error

Log Field Name	Description	Data Type	Length
action	Security action performed by DNS filter	string	16
botnetdomain	Botnet domain name	string	256
botnetip	Botnet IP address	ip	39
cat	DNS category ID	uint8	3
catdesc	DNS category description	string	64
date	Date	string	10
devid	Device ID	string	16
domainfilteridx	Domain Filter Index	uint8	3
domainfilterlist	Domain Filter List	string	512
dstintf	Destination Interface	string	32

Log Field Name	Description	Data Type	Length
dstintfrole	Destination Interface Role	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	DNS filter service error message	string	256
eventtime	Event Timestamp	uint64	20
eventtype	DNS Type (DNS query/DNS response)	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
fctuid	FortiClient ID	string	32
group	User group name	string	64
ipaddr	IP addresses from DNS response answer section	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Profile name for DNS filter	string	64
proto	Protocol number	uint8	3
qclass	Query class	string	32
qname	Query domain name	string	256
qtype	Query type description	string	32
qtypeval	Query Type Value	uint16	5
rcode		uint8	3
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface Role	string	10
srcip	Source IP	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcport	Source Port	uint16	5
sscname	Safe Search CNAME	string	256
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
time	Time	string	8
translationid		uint32	10
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name	string	256
vd	Virtual Domain Name	string	32
xid	Transaction ID	uint16	5

## 54802 - LOG\_ID\_DNS\_FTGD\_CAT\_ALLOW

**Message ID:** 54802

**Message Description:** LOG\_ID\_DNS\_FTGD\_CAT\_ALLOW

**Message Meaning:** Domain is monitored

**Type:** DNS

**Category:** DNS-RESPONSE

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by DNS filter	string	16
botnetdomain	Botnet domain name	string	256
botnetip	Botnet IP address	ip	39
cat	DNS category ID	uint8	3
catdesc	DNS category description	string	64
date	Date	string	10
devid	Device ID	string	16
domainfilteridx	Domain Filter Index	uint8	3
domainfilterlist	Domain Filter List	string	512
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface Role	string	10
dstip	Destination IP	ip	39

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
error	DNS filter service error message	string	256
eventtime	Event Timestamp	uint64	20
eventtype	DNS Type (DNS query/DNS response)	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
fctuid	FortiClient ID	string	32
group	User group name	string	64
ipaddr	IP addresses from DNS response answer section	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Profile name for DNS filter	string	64
proto	Protocol number	uint8	3
qclass	Query class	string	32
qname	Query domain name	string	256
qtype	Query type description	string	32
qtypeval	Query Type Value	uint16	5
rcode		uint8	3
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface Role	string	10
srcip	Source IP	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcport	Source Port	uint16	5
sscname	Safe Search CNAME	string	256
subtype	Log Subtype	string	20
time	Time	string	8
translationid		uint32	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name	string	256
vd	Virtual Domain Name	string	32
xid	Transaction ID	uint16	5

## 54803 - LOG\_ID\_DNS\_FTGD\_CAT\_BLOCK

**Message ID:** 54803

**Message Description:** LOG\_ID\_DNS\_FTGD\_CAT\_BLOCK

**Message Meaning:** Domain belongs to a denied category in policy

**Type:** DNS

**Category:** DNS-RESPONSE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by DNS filter	string	16
botnetdomain	Botnet domain name	string	256
botnetip	Botnet IP address	ip	39
cat	DNS category ID	uint8	3
catdesc	DNS category description	string	64
date	Date	string	10
devid	Device ID	string	16
domainfilteridx	Domain Filter Index	uint8	3
domainfilterlist	Domain Filter List	string	512
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface Role	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	DNS filter service error message	string	256

Log Field Name	Description	Data Type	Length
eventtime	Event Timestamp	uint64	20
eventtype	DNS Type (DNS query/DNS response)	string	32
exchange	Mail Exchanges from DNS response answer section	string	256
fctuid	FortiClient ID	string	32
group	User group name	string	64
ipaddr	IP addresses from DNS response answer section	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Profile name for DNS filter	string	64
proto	Protocol number	uint8	3
qclass	Query class	string	32
qname	Query domain name	string	256
qtype	Query type description	string	32
qtypeval	Query Type Value	uint16	5
rcode		uint8	3
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface Role	string	10
srcip	Source IP	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcport	Source Port	uint16	5
sscname	Safe Search CNAME	string	256
subtype	Log Subtype	string	20
time	Time	string	8
translationid		uint32	10
type	Log Type	string	16
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name	string	256
vd	Virtual Domain Name	string	32
xid	Transaction ID	uint16	5

## 54804 - LOG\_ID\_DNS\_SAFE\_SEARCH

**Message ID:** 54804

**Message Description:** LOG\_ID\_DNS\_SAFE\_SEARCH

**Message Meaning:** DNS Safe Search enforced

**Type:** DNS

**Category:** DNS-RESPONSE

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by DNS filter	string	16
botnetdomain	Botnet domain name	string	256
botnetip	Botnet IP address	ip	39
cat	DNS category ID	uint8	3
catdesc	DNS category description	string	64
date	Date	string	10
devid	Device ID	string	16
domainfilteridx	Domain Filter Index	uint8	3
domainfilterlist	Domain Filter List	string	512
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface Role	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	DNS filter service error message	string	256
eventtime	Event Timestamp	uint64	20
eventtype	DNS Type (DNS query/DNS response)	string	32

Log Field Name	Description	Data Type	Length
exchange	Mail Exchanges from DNS response answer section	string	256
fctuid	FortiClient ID	string	32
group	User group name	string	64
ipaddr	IP addresses from DNS response answer section	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Profile name for DNS filter	string	64
proto	Protocol number	uint8	3
qclass	Query class	string	32
qname	Query domain name	string	256
qtype	Query type description	string	32
qtypeval	Query Type Value	uint16	5
rcode		uint8	3
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface Role	string	10
srcip	Source IP	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcport	Source Port	uint16	5
sscname	Safe Search CNAME	string	256
subtype	Log Subtype	string	20
time	Time	string	8
translationid		uint32	10
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66



Log Field Name	Description	Data Type	Length
user	User name	string	256
vd	Virtual Domain Name	string	32
xid	Transaction ID	uint16	5

## Email

### 20480 - LOGID\_ANTISPAM\_EMAIL\_NOTIF

**Message ID:** 20480

**Message Description:** LOGID\_ANTISPAM\_EMAIL\_NOTIF

**Message Meaning:** SPAM notification

**Type:** Email

**Category:** SPAM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action of the email filter. Eg. blocked, tagged, allow	string	8
agent		string	64
attachment	Possible values: yes , no	string	3
authserver		string	64
banword	Banned word	string	128
cc	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction of packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination interface Role, ex: LAN, WAN, etc	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	the time of the event	uint64	20
eventtype	Email Filter event type	string	32

Log Field Name	Description	Data Type	Length
fctuid	FortiClient ID	string	32
fortiguardresp		string	512
from	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	128
group	User group name	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log Message	string	512
policyid	Policy ID	uint32	10
profile	Email Filter profile name	string	64
proto	Protocol number	uint8	3
recipient	Email addresses from the SMTP envelope	string	512
sender	Email addresses from the SMTP envelope	string	128
service	SMTP, POP3, IMAP, etc.	string	36
sessionid	Session ID	uint32	10
size	Email size in Bytes?	string	16
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source interface Role, ex: LAN, WAN, etc	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subject	The subject title of the email message	string	256
subtype	Log subtype	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user	User name	string	256

Log Field Name	Description	Data Type	Length
vd	Virtual Domain	string	32
vrf	Virtual router forwarding	uint8	3
webmailprovider		string	32

## 20481 - LOGID\_EMAIL\_GENERAL\_NOTIF

**Message ID:** 20481

**Message Description:** LOGID\_EMAIL\_GENERAL\_NOTIF

**Message Meaning:** Email message

**Type:** Email

**Category:** EMAIL

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action of the email filter. Eg. blocked, tagged, allow	string	8
agent		string	64
attachment	Possible values: yes , no	string	3
authserver		string	64
banword	Banned word	string	128
cc	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction of packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination interface Role, ex: LAN, WAN, etc	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	the time of the event	uint64	20
eventtype	Email Filter event type	string	32
fctuid	FortiClient ID	string	32
fortiguardresp		string	512

Log Field Name	Description	Data Type	Length
from	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	128
group	User group name	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log Message	string	512
policyid	Policy ID	uint32	10
profile	Email Filter profile name	string	64
proto	Protocol number	uint8	3
recipient	Email addresses from the SMTP envelope	string	512
sender	Email addresses from the SMTP envelope	string	128
service	SMTP, POP3, IMAP, etc.	string	36
sessionid	Session ID	uint32	10
size	Email size in Bytes?	string	16
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source interface Role, ex: LAN, WAN, etc	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subject	The subject title of the email message	string	256
subtype	Log subtype	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user	User name	string	256
vd	Virtual Domain	string	32
vrf	Virtual router forwarding	uint8	3
webmailprovider		string	32

## 20482 - LOGID\_ANTISPAM\_EMAIL\_BWORD\_NOTIF

**Message ID:** 20482

**Message Description:** LOGID\_ANTISPAM\_EMAIL\_BWORD\_NOTIF

**Message Meaning:** Banned word notification

**Type:** Email

**Category:** BANNEDWORD

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action of the email filter. Eg. blocked, tagged, allow	string	8
agent		string	64
attachment	Possible values: yes , no	string	3
authserver		string	64
banword	Banned word	string	128
cc	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction of packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination interface Role, ex: LAN, WAN, etc	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	the time of the event	uint64	20
eventtype	Email Filter event type	string	32
fctuid	FortiClient ID	string	32
fortiguardresp		string	512
from	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	128
group	User group name	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log Message	string	512

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	Email Filter profile name	string	64
proto	Protocol number	uint8	3
recipient	Email addresses from the SMTP envelope	string	512
sender	Email addresses from the SMTP envelope	string	128
service	SMTP, POP3, IMAP, etc.	string	36
sessionid	Session ID	uint32	10
size	Email size in Bytes?	string	16
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source interface Role, ex: LAN, WAN, etc	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subject	The subject title of the email message	string	256
subtype	Log subtype	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user	User name	string	256
vd	Virtual Domain	string	32
vrf	Virtual router forwarding	uint8	3
webmailprovider		string	32

## 20509 - LOGID\_ANTISPAM\_FTGD\_ERR

**Message ID:** 20509

**Message Description:** LOGID\_ANTISPAM\_FTGD\_ERR

**Message Meaning:** FortiGuard error message

**Type:** Email

**Category:** FTGD\_ERR**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action of the email filter. Eg. blocked, tagged, allow	string	8
agent		string	64
attachment	Possible values: yes , no	string	3
authserver		string	64
banword	Banned word	string	128
cc	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction of packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination interface Role, ex: LAN, WAN, etc	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	the time of the event	uint64	20
eventtype	Email Filter event type	string	32
fctuid	FortiClient ID	string	32
fortiguardresp		string	512
from	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	128
group	User group name	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log Message	string	512
policyid	Policy ID	uint32	10
profile	Email Filter profile name	string	64
proto	Protocol number	uint8	3
recipient	Email addresses from the SMTP envelope	string	512
sender	Email addresses from the SMTP envelope	string	128

Log Field Name	Description	Data Type	Length
service	SMTP, POP3, IMAP, etc.	string	36
sessionid	Session ID	uint32	10
size	Email size in Bytes?	string	16
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source interface Role, ex: LAN, WAN, etc	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subject	The subject title of the email message	string	256
subtype	Log subtype	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user	User name	string	256
vd	Virtual Domain	string	32
vrf	Virtual router forwarding	uint8	3
webmailprovider		string	32

## 20510 - LOGID\_ANTISPAM\_EMAIL\_WEBMAIL\_NOTIF

**Message ID:** 20510

**Message Description:** LOGID\_ANTISPAM\_EMAIL\_WEBMAIL\_NOTIF

**Message Meaning:** Webmail message

**Type:** Email

**Category:** WEBMAIL

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action of the email filter. Eg. blocked, tagged, allow	string	8



Log Field Name	Description	Data Type	Length
agent		string	64
attachment	Possible values: yes , no	string	3
authserver		string	64
banword	Banned word	string	128
cc	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction of packets	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination interface Role, ex: LAN, WAN, etc	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	the time of the event	uint64	20
eventtype	Email Filter event type	string	32
fctuid	FortiClient ID	string	32
fortiguardresp		string	512
from	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	128
group	User group name	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log Message	string	512
policyid	Policy ID	uint32	10
profile	Email Filter profile name	string	64
proto	Protocol number	uint8	3
recipient	Email addresses from the SMTP envelope	string	512
sender	Email addresses from the SMTP envelope	string	128
service	SMTP, POP3, IMAP, etc.	string	36
sessionid	Session ID	uint32	10
size	Email size in Bytes?	string	16

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source interface Role, ex: LAN, WAN, etc	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subject	The subject title of the email message	string	256
subtype	Log subtype	string	20
time	Time	string	8
to	Email address(es) from the Email Headers (IMAP/POP3/SMTP)	string	512
type	Log type	string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user	User name	string	256
vd	Virtual Domain	string	32
vrf	Virtual router forwarding	uint8	3
webmailprovider		string	32

## Event

### 20002 - LOG\_ID\_DOMAIN\_UNRESOLVABLE

**Message ID:** 20002

**Message Description:** LOG\_ID\_DOMAIN\_UNRESOLVABLE

**Message Meaning:** Domain name of alert email sender unresolvable

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 20003 - LOG\_ID\_MAIL\_SENT\_FAIL

**Message ID:** 20003

**Message Description:** LOG\_ID\_MAIL\_SENT\_FAIL

**Message Meaning:** Alert email send status failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
count	Count	uint32	10

## 20004 - LOG\_ID\_POLICY\_TOO\_BIG

**Message ID:** 20004

**Message Description:** LOG\_ID\_POLICY\_TOO\_BIG

**Message Meaning:** Policy too big for installation

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
status	Status	string	23
msg	Log Message	string	4096

## 20005 - LOG\_ID\_PPP\_LINK\_UP

**Message ID:** 20005

**Message Description:** LOG\_ID\_PPP\_LINK\_UP

**Message Meaning:** Modem PPP link up

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20006 - LOG\_ID\_PPP\_LINK\_DOWN

**Message ID:** 20006

**Message Description:** LOG\_ID\_PPP\_LINK\_DOWN

**Message Meaning:** Modem PPP link down

**Type:** Event**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20007 - LOG\_ID\_SOCKET\_EXHAUSTED

**Message ID:** 20007**Message Description:** LOG\_ID\_SOCKET\_EXHAUSTED**Message Meaning:** NAT port exhausted**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
service	Name of Service	string	64
proto	Protocol Number	uint8	3
vrf		uint8	3
srcip	Source IP	ip	39
srcport	Source port	uint16	5
nat	NAT IP Address	ip	39
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5

## 20008 - LOG\_ID\_POLICY6\_TOO\_BIG

**Message ID:** 20008

**Message Description:** LOG\_ID\_POLICY6\_TOO\_BIG

**Message Meaning:** IPv6 policy too big for installation

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
status	Status	string	23
msg	Log Message	string	4096

## 20010 - LOG\_ID\_KERNEL\_ERROR

**Message ID:** 20010

**Message Description:** LOG\_ID\_KERNEL\_ERROR

**Message Meaning:** Kernel error

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096



## 20016 - LOG\_ID\_MODEM\_EXCEED\_REDIAL\_COUNT

**Message ID:** 20016

**Message Description:** LOG\_ID\_MODEM\_EXCEED\_REDIAL\_COUNT

**Message Meaning:** Modem exceeded redial limit

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20017 - LOG\_ID\_MODEM\_FAIL\_TO\_OPEN

**Message ID:** 20017

**Message Description:** LOG\_ID\_MODEM\_FAIL\_TO\_OPEN

**Message Meaning:** Modem failed to open

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20020 - LOG\_ID\_MODEM\_USB\_DETECTED

**Message ID:** 20020

**Message Description:** LOG\_ID\_MODEM\_USB\_DETECTED

**Message Meaning:** USB modem detected

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20021 - LOG\_ID\_MAIL\_RESENT

**Message ID:** 20021

**Message Description:** LOG\_ID\_MAIL\_RESENT

**Message Meaning:** Alert email resent

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
count	Count	uint32	10

## 20022 - LOG\_ID\_MODEM\_USB\_REMOVED

**Message ID:** 20022

**Message Description:** LOG\_ID\_MODEM\_USB\_REMOVED

**Message Meaning:** USB modem removed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20023 - LOG\_ID\_MODEM\_USBLTE\_DETECTED

**Message ID:** 20023**Message Description:** LOG\_ID\_MODEM\_USBLTE\_DETECTED**Message Meaning:** USB LTE modem detected**Type:** Event**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20024 - LOG\_ID\_MODEM\_USBLTE\_REMOVED

**Message ID:** 20024

**Message Description:** LOG\_ID\_MODEM\_USBLTE\_REMOVED

**Message Meaning:** USB LTE modem removed

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20025 - LOG\_ID\_REPORTD\_REPORT\_SUCCESS

**Message ID:** 20025

**Message Description:** LOG\_ID\_REPORTD\_REPORT\_SUCCESS

**Message Meaning:** Report generated successfully

**Type:** Event

**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
file	Report file full path	string	256
filesize	Report File Size in Bytes	uint32	10
datarange	Data range for reports	string	50
reporttype	Report Type	string	20
processtime	Process time for reports	uint32	10

## 20026 - LOG\_ID\_REPORTD\_REPORT\_FAILURE

**Message ID:** 20026**Message Description:** LOG\_ID\_REPORTD\_REPORT\_FAILURE**Message Meaning:** Report generation failed**Type:** Event**Category:** SYSTEM**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20028 - LOG\_ID\_REPORT\_RECREATE\_DB

**Message ID:** 20028

**Message Description:** LOG\_ID\_REPORT\_RECREATE\_DB

**Message Meaning:** Report database recreated

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20031 - LOG\_ID\_RAD\_OUT\_OF\_MEM

**Message ID:** 20031

**Message Description:** LOG\_ID\_RAD\_OUT\_OF\_MEM

**Message Meaning:** RADVD out of memory

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20032 - LOG\_ID\_RAD\_NOT\_FOUND

**Message ID:** 20032

**Message Description:** LOG\_ID\_RAD\_NOT\_FOUND

**Message Meaning:** RADVD interface not found

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8



Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20033 - LOG\_ID\_RAD\_MOBILE\_IPV6

**Message ID:** 20033

**Message Description:** LOG\_ID\_RAD\_MOBILE\_IPV6

**Message Meaning:** RADVD mobile IPv6 extensions used

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20034 - LOG\_ID\_RAD\_IPV6\_OUT\_OF\_RANGE

**Message ID:** 20034

**Message Description:** LOG\_ID\_RAD\_IPV6\_OUT\_OF\_RANGE

**Message Meaning:** RADVD mobile IPv6 MinRtrAdvInterval out of range

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20035 - LOG\_ID\_RAD\_MIN\_OUT\_OF\_RANGE

**Message ID:** 20035

**Message Description:** LOG\_ID\_RAD\_MIN\_OUT\_OF\_RANGE

**Message Meaning:** RADVD MinRtrAdvInterval out of range

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20036 - LOG\_ID\_RAD\_MAX\_OUT\_OF\_RANGE

**Message ID:** 20036

**Message Description:** LOG\_ID\_RAD\_MAX\_OUT\_OF\_RANGE

**Message Meaning:** RADVD mobile IPv6 MaxRtrAdvInterval out of range

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20037 - LOG\_ID\_RAD\_MAX\_ADV\_OUT\_OF\_RANGE

**Message ID:** 20037

**Message Description:** LOG\_ID\_RAD\_MAX\_ADV\_OUT\_OF\_RANGE

**Message Meaning:** RADVD MaxRtrAdvInterval out of range

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20039 - LOG\_ID\_RAD\_MTU\_TOO\_SMALL

**Message ID:** 20039

**Message Description:** LOG\_ID\_RAD\_MTU\_TOO\_SMALL

**Message Meaning:** RADVD AdvLinkMTU too small

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20040 - LOG\_ID\_RAD\_TIME\_TOO\_SMALL

**Message ID:** 20040

**Message Description:** LOG\_ID\_RAD\_TIME\_TOO\_SMALL

**Message Meaning:** RADVD AdvReachableTime too small

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20041 - LOG\_ID\_RAD\_HOP\_OUT\_OF\_RANGE

**Message ID:** 20041

**Message Description:** LOG\_ID\_RAD\_HOP\_OUT\_OF\_RANGE

**Message Meaning:** RADVD AdvCurHopLimit too big

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20042 - LOG\_ID\_RAD\_DFT\_HOP\_OUT\_OF\_RANGE

**Message ID:** 20042

**Message Description:** LOG\_ID\_RAD\_DFT\_HOP\_OUT\_OF\_RANGE

**Message Meaning:** RADVD AdvCurHopLimit out of range

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20043 - LOG\_ID\_RAD\_AGENT\_OUT\_OF\_RANGE

**Message ID:** 20043

**Message Description:** LOG\_ID\_RAD\_AGENT\_OUT\_OF\_RANGE

**Message Meaning:** RADVD HomeAgentLifetime out of range

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20044 - LOG\_ID\_RAD\_AGENT\_FLAG\_NOT\_SET

**Message ID:** 20044

**Message Description:** LOG\_ID\_RAD\_AGENT\_FLAG\_NOT\_SET

**Message Meaning:** RADVD AdvHomeAgentFlag not set

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20045 - LOG\_ID\_RAD\_PREFIX\_TOO\_LONG

**Message ID:** 20045

**Message Description:** LOG\_ID\_RAD\_PREFIX\_TOO\_LONG

**Message Meaning:** RADVD invalid prefix length

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8



Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20046 - LOG\_ID\_RAD\_PREF\_TIME\_TOO\_SMALL

**Message ID:** 20046

**Message Description:** LOG\_ID\_RAD\_PREF\_TIME\_TOO\_SMALL

**Message Meaning:** RADVD AdvValidLifetime less than AdvPreferredLifetime

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20047 - LOG\_ID\_RAD\_FAIL\_IPV6\_SOCKET

**Message ID:** 20047

**Message Description:** LOG\_ID\_RAD\_FAIL\_IPV6\_SOCKET

**Message Meaning:** RADVD failed to create an IPv6 socket

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20048 - LOG\_ID\_RAD\_FAIL\_OPT\_IPV6\_PKTINFO

**Message ID:** 20048

**Message Description:** LOG\_ID\_RAD\_FAIL\_OPT\_IPV6\_PKTINFO

**Message Meaning:** RADVD failed to set IPv6 packet info

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20049 - LOG\_ID\_RAD\_FAIL\_OPT\_IPV6\_CHECKSUM

**Message ID:** 20049

**Message Description:** LOG\_ID\_RAD\_FAIL\_OPT\_IPV6\_CHECKSUM

**Message Meaning:** RADVD failed to set IPv6 checksum

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20050 - LOG\_ID\_RAD\_FAIL\_OPT\_IPV6\_UNICAST\_HOPS

**Message ID:** 20050

**Message Description:** LOG\_ID\_RAD\_FAIL\_OPT\_IPV6\_UNICAST\_HOPS

**Message Meaning:** RADVD failed to set IPv6 unicast hops

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20051 - LOG\_ID\_RAD\_FAIL\_OPT\_IPV6\_MULTICAST\_HOPS

**Message ID:** 20051

**Message Description:** LOG\_ID\_RAD\_FAIL\_OPT\_IPV6\_MULTICAST\_HOPS

**Message Meaning:** RADVD failed to set IPv6 multicast hops

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20052 - LOG\_ID\_RAD\_FAIL\_OPT\_IPV6\_HOPLIMIT

**Message ID:** 20052

**Message Description:** LOG\_ID\_RAD\_FAIL\_OPT\_IPV6\_HOPLIMIT

**Message Meaning:** RADVD failed to set IPv6 hop limit

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20053 - LOG\_ID\_RAD\_FAIL\_OPT\_IPPROTO\_ICMPV6

**Message ID:** 20053

**Message Description:** LOG\_ID\_RAD\_FAIL\_OPT\_IPPROTO\_ICMPV6

**Message Meaning:** RADVD failed to set ICMPv6 filter

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20054 - LOG\_ID\_RAD\_EXIT\_BY\_SIGNAL

**Message ID:** 20054

**Message Description:** LOG\_ID\_RAD\_EXIT\_BY\_SIGNAL

**Message Meaning:** RADVD exited due to received signal

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20055 - LOG\_ID\_RAD\_FAIL\_CMDB\_QUERY

**Message ID:** 20055

**Message Description:** LOG\_ID\_RAD\_FAIL\_CMDB\_QUERY

**Message Meaning:** RADVD interface query creation failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20056 - LOG\_ID\_RAD\_FAIL\_CMDB\_FOR\_EACH

**Message ID:** 20056

**Message Description:** LOG\_ID\_RAD\_FAIL\_CMDB\_FOR\_EACH

**Message Meaning:** RADVD query error

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20057 - LOG\_ID\_RAD\_FAIL\_FIND\_VIRT\_INTF

**Message ID:** 20057

**Message Description:** LOG\_ID\_RAD\_FAIL\_FIND\_VIRT\_INTF

**Message Meaning:** RADVD virtual interface not found

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8



Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20058 - LOG\_ID\_RAD\_UNLOAD\_INTF

**Message ID:** 20058

**Message Description:** LOG\_ID\_RAD\_UNLOAD\_INTF

**Message Meaning:** RADVD unloaded interface

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20061 - LOG\_ID\_RAD\_INV\_ICMPV6\_TYPE

**Message ID:** 20061

**Message Description:** LOG\_ID\_RAD\_INV\_ICMPV6\_TYPE

**Message Meaning:** RADVD received unwanted ICMPv6 packet

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20062 - LOG\_ID\_RAD\_INV\_ICMPV6\_RA\_LEN

**Message ID:** 20062

**Message Description:** LOG\_ID\_RAD\_INV\_ICMPV6\_RA\_LEN

**Message Meaning:** RADVD received ICMPv6 RA packet with invalid length

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20063 - LOG\_ID\_RAD\_ICMPV6\_NO\_SRC\_ADDR

**Message ID:** 20063

**Message Description:** LOG\_ID\_RAD\_ICMPV6\_NO\_SRC\_ADDR

**Message Meaning:** RADVD received ICMPv6 RA packet with non-link local source address

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20064 - LOG\_ID\_RAD\_INV\_ICMPV6\_RS\_LEN

**Message ID:** 20064

**Message Description:** LOG\_ID\_RAD\_INV\_ICMPV6\_RS\_LEN

**Message Meaning:** RADVD received ICMPv6 RS packet with invalid length

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20065 - LOG\_ID\_RAD\_INV\_ICMPV6\_CODE

**Message ID:** 20065

**Message Description:** LOG\_ID\_RAD\_INV\_ICMPV6\_CODE

**Message Meaning:** RADVD received ICMPv6 RS/RA packet with invalid code

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20066 - LOG\_ID\_RAD\_INV\_ICMPV6\_HOP

**Message ID:** 20066

**Message Description:** LOG\_ID\_RAD\_INV\_ICMPV6\_HOP

**Message Meaning:** RADVD received ICMPv6 RS/RA packet with invalid hop limit

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20067 - LOG\_ID\_RAD\_MISMATCH\_HOP

**Message ID:** 20067

**Message Description:** LOG\_ID\_RAD\_MISMATCH\_HOP

**Message Meaning:** RADVD local AdvCurHopLimit disagrees with remote site

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20068 - LOG\_ID\_RAD\_MISMATCH\_MGR\_FLAG

**Message ID:** 20068

**Message Description:** LOG\_ID\_RAD\_MISMATCH\_MGR\_FLAG

**Message Meaning:** RADVD local AdvManagedFlag disagrees with remote site

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20069 - LOG\_ID\_RAD\_MISMATCH\_OTH\_FLAG

**Message ID:** 20069

**Message Description:** LOG\_ID\_RAD\_MISMATCH\_OTH\_FLAG

**Message Meaning:** RADVD local AdvOtherConfigFlag disagrees with remote site

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20070 - LOG\_ID\_RAD\_MISMATCH\_TIME

**Message ID:** 20070

**Message Description:** LOG\_ID\_RAD\_MISMATCH\_TIME

**Message Meaning:** RADVD local AdvReachableTime disagrees with remote site

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20071 - LOG\_ID\_RAD\_MISMATCH\_TIMER

**Message ID:** 20071

**Message Description:** LOG\_ID\_RAD\_MISMATCH\_TIMER

**Message Meaning:** RADVD local AdvRetransTimer disagrees with remote site

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8



Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20072 - LOG\_ID\_RAD\_EXTRA\_DATA

**Message ID:** 20072

**Message Description:** LOG\_ID\_RAD\_EXTRA\_DATA

**Message Meaning:** RADVD extra data in RA packet found

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20073 - LOG\_ID\_RAD\_NO\_OPT\_DATA

**Message ID:** 20073

**Message Description:** LOG\_ID\_RAD\_NO\_OPT\_DATA

**Message Meaning:** RADVD RA packet option length zero

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20074 - LOG\_ID\_RAD\_INV\_OPT\_LEN

**Message ID:** 20074

**Message Description:** LOG\_ID\_RAD\_INV\_OPT\_LEN

**Message Meaning:** RADVD RA packet option length greater than total length

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20075 - LOG\_ID\_RAD\_MISMATCH\_MTU

**Message ID:** 20075

**Message Description:** LOG\_ID\_RAD\_MISMATCH\_MTU

**Message Meaning:** RADVD local AdvLinkMTU disagrees with remote site

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20077 - LOG\_ID\_RAD\_MISMATCH\_PREF\_TIME

**Message ID:** 20077

**Message Description:** LOG\_ID\_RAD\_MISMATCH\_PREF\_TIME

**Message Meaning:** Interface AdvPreferredLifetime on our interface does not agree with a remote site

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20078 - LOG\_ID\_RAD\_INV\_OPT

**Message ID:** 20078

**Message Description:** LOG\_ID\_RAD\_INV\_OPT

**Message Meaning:** RADVD found invalid option in RA packet from remote site

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20080 - LOG\_ID\_RAD\_FAIL\_TO\_RCV

**Message ID:** 20080

**Message Description:** LOG\_ID\_RAD\_FAIL\_TO\_RCV

**Message Meaning:** RADVD receive message failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20081 - LOG\_ID\_RAD\_INV\_HOP

**Message ID:** 20081

**Message Description:** LOG\_ID\_RAD\_INV\_HOP

**Message Meaning:** RADVD received invalid IPv6 hop limit

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20082 - LOG\_ID\_RAD\_INV\_PKTINFO

**Message ID:** 20082

**Message Description:** LOG\_ID\_RAD\_INV\_PKTINFO

**Message Meaning:** RADVD received invalid IPv6 packet info

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20083 - LOG\_ID\_RAD\_FAIL\_TO\_CHECK

**Message ID:** 20083

**Message Description:** LOG\_ID\_RAD\_FAIL\_TO\_CHECK

**Message Meaning:** RADVD all-routers membership check failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20084 - LOG\_ID\_RAD\_FAIL\_TO\_SEND

**Message ID:** 20084

**Message Description:** LOG\_ID\_RAD\_FAIL\_TO\_SEND

**Message Meaning:** RADVD send message failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20085 - LOG\_ID\_SESSION\_CLASH

**Message ID:** 20085

**Message Description:** LOG\_ID\_SESSION\_CLASH

**Message Meaning:** Session clashed

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8



Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
proto	Protocol Number	uint8	3
trace_id		string	32

## 20090 - LOG\_ID\_INTF\_LINK\_STA\_CHG

**Message ID:** 20090

**Message Description:** LOG\_ID\_INTF\_LINK\_STA\_CHG

**Message Meaning:** Interface link status changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
intf	Interface	string	16

## 20099 - LOG\_ID\_INTF\_STA\_CHG

**Message ID:** 20099

**Message Description:** LOG\_ID\_INTF\_STA\_CHG

**Message Meaning:** Interface status changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 20100 - LOG\_ID\_WEB\_CAT\_UPDATED

**Message ID:** 20100

**Message Description:** LOG\_ID\_WEB\_CAT\_UPDATED

**Message Meaning:** FortiGuard web filter category list updated

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20101 - LOG\_ID\_WEB\_LIC\_EXPIRE

**Message ID:** 20101

**Message Description:** LOG\_ID\_WEB\_LIC\_EXPIRE

**Message Meaning:** FortiGuard web filter license expiring

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20102 - LOG\_ID\_SPAM\_LIC\_EXPIRE

**Message ID:** 20102

**Message Description:** LOG\_ID\_SPAM\_LIC\_EXPIRE

**Message Meaning:** FortiGuard antispam license expiring

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20103 - LOG\_ID\_AV\_LIC\_EXPIRE

**Message ID:** 20103

**Message Description:** LOG\_ID\_AV\_LIC\_EXPIRE

**Message Meaning:** FortiGuard antivirus license expiring

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20104 - LOG\_ID\_IPS\_LIC\_EXPIRE

**Message ID:** 20104

**Message Description:** LOG\_ID\_IPS\_LIC\_EXPIRE

**Message Meaning:** FortiGuard IPS license expiring

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20107 - LOG\_ID\_LOG\_UPLOAD\_ERR

**Message ID:** 20107

**Message Description:** LOG\_ID\_LOG\_UPLOAD\_ERR

**Message Meaning:** Log upload error

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096
error	Error Reason for Log Upload to Forticloud	string	256
server	Server IP Address	string	64
port	Port Number	uint16	5

## 20108 - LOG\_ID\_LOG\_UPLOAD\_DONE

**Message ID:** 20108

**Message Description:** LOG\_ID\_LOG\_UPLOAD\_DONE

**Message Meaning:** Log upload completed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
server	Server IP Address	string	64
port	Port Number	uint16	5

## 20109 - LOG\_ID\_WEB\_LIC\_EXPIRED

**Message ID:** 20109

**Message Description:** LOG\_ID\_WEB\_LIC\_EXPIRED

**Message Meaning:** FortiGuard web filter license expired

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20113 - LOG\_ID\_IPSA\_DOWNLOAD\_FAIL

**Message ID:** 20113

**Message Description:** LOG\_ID\_IPSA\_DOWNLOAD\_FAIL

**Message Meaning:** IPSA database download failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Error



Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20114 - LOG\_ID\_IPSA\_SELFTEST\_FAIL

**Message ID:** 20114

**Message Description:** LOG\_ID\_IPSA\_SELFTEST\_FAIL

**Message Meaning:** IPSA disabled: self test failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20115 - LOG\_ID\_IPSA\_STATUSUPD\_FAIL

**Message ID:** 20115

**Message Description:** LOG\_ID\_IPSA\_STATUSUPD\_FAIL

**Message Meaning:** IPSA driver update failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20116 - LOG\_ID\_SPAM\_LIC\_EXPIRED

**Message ID:** 20116

**Message Description:** LOG\_ID\_SPAM\_LIC\_EXPIRED

**Message Meaning:** FortiGuard antispam license expired

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20117 - LOG\_ID\_AV\_LIC\_EXPIRED

**Message ID:** 20117**Message Description:** LOG\_ID\_AV\_LIC\_EXPIRED**Message Meaning:** FortiGuard antivirus license expired**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20118 - LOG\_ID\_WEBF\_STATUS\_REACH

**Message ID:** 20118

**Message Description:** LOG\_ID\_WEBF\_STATUS\_REACH

**Message Meaning:** FortiGuard webfilter reachable

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20119 - LOG\_ID\_WEBF\_STATUS\_UNREACH

**Message ID:** 20119

**Message Description:** LOG\_ID\_WEBF\_STATUS\_UNREACH

**Message Meaning:** FortiGuard webfilter unreachable

**Type:** Event

**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20200 - LOG\_ID\_FIPS\_SELF\_TEST

**Message ID:** 20200**Message Description:** LOG\_ID\_FIPS\_SELF\_TEST**Message Meaning:** FIPS CC self-test initiated**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 20201 - LOG\_ID\_FIPS\_SELF\_ALL\_TEST

**Message ID:** 20201

**Message Description:** LOG\_ID\_FIPS\_SELF\_ALL\_TEST

**Message Meaning:** FIPS ALL CC self-tests initiated

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 20202 - LOG\_ID\_DISK\_FORMAT\_ERROR

**Message ID:** 20202

**Message Description:** LOG\_ID\_DISK\_FORMAT\_ERROR

**Message Meaning:** Disk partitioning or formatting Error

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20203 - LOG\_ID\_DAEMON\_SHUTDOWN

**Message ID:** 20203

**Message Description:** LOG\_ID\_DAEMON\_SHUTDOWN

**Message Meaning:** Daemon shutdown

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
daemon	Daemon Name	string	32
pid	Process ID	uint32	10

## 20204 - LOG\_ID\_DAEMON\_START

**Message ID:** 20204

**Message Description:** LOG\_ID\_DAEMON\_START

**Message Meaning:** Daemon started

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32



Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
daemon	Daemon Name	string	32
pid	Process ID	uint32	10

## 20205 - LOG\_ID\_DISK\_FORMAT\_REQ

**Message ID:** 20205

**Message Description:** LOG\_ID\_DISK\_FORMAT\_REQ

**Message Meaning:** Format disk requested

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 20206 - LOG\_ID\_DISK\_SCAN\_REQ

**Message ID:** 20206

**Message Description:** LOG\_ID\_DISK\_SCAN\_REQ

**Message Meaning:** Scan disk requested

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 20207 - LOG\_ID\_RAD\_MISMATCH\_VALID\_TIME

**Message ID:** 20207

**Message Description:** LOG\_ID\_RAD\_MISMATCH\_VALID\_TIME

**Message Meaning:** RADVD local AdvValidLifetime disagrees with remote site

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20208 - LOG\_ID\_ZOMBIE\_DAEMON\_CLEANUP

**Message ID:** 20208

**Message Description:** LOG\_ID\_ZOMBIE\_DAEMON\_CLEANUP

**Message Meaning:** Zombie daemon cleanup

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
daemon	Daemon Name	string	32
pid	Process ID	uint32	10

## 20209 - LOG\_ID\_DISK\_UNAVAIL

**Message ID:** 20209

**Message Description:** LOG\_ID\_DISK\_UNAVAIL

**Message Meaning:** Disk unavailable

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20210 - LOG\_ID\_DISK\_TRIM\_START

**Message ID:** 20210

**Message Description:** LOG\_ID\_DISK\_TRIM\_START

**Message Meaning:** SSD TRIM started

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 20211 - LOG\_ID\_DISK\_TRIM\_END

**Message ID:** 20211

**Message Description:** LOG\_ID\_DISK\_TRIM\_END

**Message Meaning:** SSD TRIM finished

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 20212 - LOG\_ID\_DISK\_SCAN\_NEEDED

**Message ID:** 20212

**Message Description:** LOG\_ID\_DISK\_SCAN\_NEEDED

**Message Meaning:** Disk scan is needed

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20213 - LOG\_ID\_DISK\_LOG\_CORRUPTED

**Message ID:** 20213

**Message Description:** LOG\_ID\_DISK\_LOG\_CORRUPTED

**Message Meaning:** Log file on disk is corrupted

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20220 - LOGID\_EVENT\_SHAPER\_OUTBOUND\_MAXED\_OUT

**Message ID:** 20220

**Message Description:** LOGID\_EVENT\_SHAPER\_OUTBOUND\_MAXED\_OUT

**Message Meaning:** Outbound bandwidth rate exceeded

**Type:** Event

**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
intf	Interface	string	16
limit	Virtual Domain Resource Limit	uint32	10

## 20221 - LOGID\_EVENT\_SHAPER\_INBOUND\_MAXED\_OUT

**Message ID:** 20221**Message Description:** LOGID\_EVENT\_SHAPER\_INBOUND\_MAXED\_OUT**Message Meaning:** Inbound bandwidth rate exceeded**Type:** Event**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11



Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
intf	Interface	string	16
limit	Virtual Domain Resource Limit	uint32	10

## 20230 - LOG\_ID\_SYS\_SECURITY\_WRITE\_VIOLATION

**Message ID:** 20230

**Message Description:** LOG\_ID\_SYS\_SECURITY\_WRITE\_VIOLATION

**Message Meaning:** Write Permission Violation

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 20231 - LOG\_ID\_SYS\_SECURITY\_HARDLINK\_VIOLATION

**Message ID:** 20231

**Message Description:** LOG\_ID\_SYS\_SECURITY\_HARDLINK\_VIOLATION**Message Meaning:** Hard Link Creation Violation**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 20232 - LOG\_ID\_SYS\_SECURITY\_LOAD\_MODULE\_VIOLATION

**Message ID:** 20232**Message Description:** LOG\_ID\_SYS\_SECURITY\_LOAD\_MODULE\_VIOLATION**Message Meaning:** Load Kernel/Kernel Module/Firmware Violation**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 20233 - LOG\_ID\_SYS\_SECURITY\_FILE\_HASH\_MISSING

**Message ID:** 20233

**Message Description:** LOG\_ID\_SYS\_SECURITY\_FILE\_HASH\_MISSING

**Message Meaning:** Integrity check of Run/loading Executable File failed without Integrity measure

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 20234 - LOG\_ID\_SYS\_SECURITY\_FILE\_HASH\_MISMATCH

**Message ID:** 20234

**Message Description:** LOG\_ID\_SYS\_SECURITY\_FILE\_HASH\_MISMATCH

**Message Meaning:** Integrity check of Run/loading Executable File failed with mismatched measure

**Type:** Event**Category:** SYSTEM**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 20300 - LOG\_ID\_BGP\_NB\_STAT\_CHG

**Message ID:** 20300**Message Description:** LOG\_ID\_BGP\_NB\_STAT\_CHG**Message Meaning:** BGP neighbor status changed**Type:** Event**Category:** ROUTER**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20301 - LOG\_ID\_VZ\_LOG

**Message ID:** 20301

**Message Description:** LOG\_ID\_VZ\_LOG

**Message Meaning:** Routing log

**Type:** Event

**Category:** ROUTER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20302 - LOG\_ID\_OSPF\_NB\_STAT\_CHG

**Message ID:** 20302

**Message Description:** LOG\_ID\_OSPF\_NB\_STAT\_CHG

**Message Meaning:** OSPF neighbor status changed

**Type:** Event**Category:** ROUTER**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20303 - LOG\_ID\_OSPF6\_NB\_STAT\_CHG

**Message ID:** 20303**Message Description:** LOG\_ID\_OSPF6\_NB\_STAT\_CHG**Message Meaning:** OSPF6 neighbor status changed**Type:** Event**Category:** ROUTER**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 20401 - LOG\_ID\_ROUTER\_CLEAR

**Message ID:** 20401

**Message Description:** LOG\_ID\_ROUTER\_CLEAR

**Message Meaning:** Router cleared

**Type:** Event

**Category:** ROUTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65

## 22000 - LOG\_ID\_INV\_PKT\_LEN

**Message ID:** 22000

**Message Description:** LOG\_ID\_INV\_PKT\_LEN

**Message Meaning:** Packet length mismatch

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22001 - LOG\_ID\_UNSUPPORTED\_PROT\_VER

**Message ID:** 22001

**Message Description:** LOG\_ID\_UNSUPPORTED\_PROT\_VER

**Message Meaning:** Protocol version unsupported

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8



Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22002 - LOG\_ID\_INV\_REQ\_TYPE

**Message ID:** 22002

**Message Description:** LOG\_ID\_INV\_REQ\_TYPE

**Message Meaning:** Request type not supported

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22003 - LOG\_ID\_FAIL\_SET\_SIG\_HANDLER

**Message ID:** 22003

**Message Description:** LOG\_ID\_FAIL\_SET\_SIG\_HANDLER

**Message Meaning:** Signal handler setup failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22004 - LOG\_ID\_FAIL\_CREATE\_SOCKET

**Message ID:** 22004

**Message Description:** LOG\_ID\_FAIL\_CREATE\_SOCKET

**Message Meaning:** Socket creation failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 22005 - LOG\_ID\_FAIL\_CREATE\_SOCKET\_RETRY

**Message ID:** 22005

**Message Description:** LOG\_ID\_FAIL\_CREATE\_SOCKET\_RETRY

**Message Meaning:** Socket creation retry failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 22006 - LOG\_ID\_FAIL\_REG\_CMDB\_EVENT

**Message ID:** 22006

**Message Description:** LOG\_ID\_FAIL\_REG\_CMDB\_EVENT

**Message Meaning:** Registration for CMDB events failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22009 - LOG\_ID\_FAIL\_FIND\_AV\_PROFILE

**Message ID:** 22009

**Message Description:** LOG\_ID\_FAIL\_FIND\_AV\_PROFILE

**Message Meaning:** AntiVirus profile not found

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
name	Display Name of the Connection	string	128

## 22010 - LOG\_ID\_SENDTO\_FAIL

**Message ID:** 22010

**Message Description:** LOG\_ID\_SENDTO\_FAIL

**Message Meaning:** URL filter packet send failure

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
process	Process	string	4096
reason	Reason	string	256

## 22011 - LOG\_ID\_ENTER\_MEM\_CONSERVE\_MODE

**Message ID:** 22011

**Message Description:** LOG\_ID\_ENTER\_MEM\_CONSERVE\_MODE

**Message Meaning:** Memory conserve mode entered

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
service	Name of Service	string	64
conserve	Flag for Conserve Mode	string	32
total	Total	uint32	10
used	Number of Used IPs	uint32	10

Log Field Name	Description	Data Type	Length
red		string	32
green	Green threshold for conserve mode	string	32

## 22012 - LOG\_ID\_LEAVE\_MEM\_CONSERVE\_MODE

**Message ID:** 22012

**Message Description:** LOG\_ID\_LEAVE\_MEM\_CONSERVE\_MODE

**Message Meaning:** Memory conserve mode exited

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
service	Name of Service	string	64
conserve	Flag for Conserve Mode	string	32
total	Total	uint32	10
used	Number of Used IPs	uint32	10
red		string	32
green	Green threshold for conserve mode	string	32

## 22013 - LOG\_ID\_IPPOOLPBA\_BLOCK\_EXHAUSTED

**Message ID:** 22013

**Message Description:** LOG\_ID\_IPPOOLPBA\_BLOCK\_EXHAUSTED

**Message Meaning:** IP pool PBA block exhausted

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
saddr	Source Address IP	string	80
poolname	IP Pool Name	string	36

## 22014 - LOG\_ID\_IPPOOLPBA\_NATIP\_EXHAUSTED

**Message ID:** 22014

**Message Description:** LOG\_ID\_IPPOOLPBA\_NATIP\_EXHAUSTED

**Message Meaning:** IP pool PBA NAT IP exhausted

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert



Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
saddr	Source Address IP	string	80
poolname	IP Pool Name	string	36

## 22015 - LOG\_ID\_IPPOOLPBA\_CREATE

**Message ID:** 22015

**Message Description:** LOG\_ID\_IPPOOLPBA\_CREATE

**Message Meaning:** IP pool PBA created

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
nat	NAT IP Address	ip	39
saddr	Source Address IP	string	80
poolname	IP Pool Name	string	36
portbegin	Port Number to Begin	uint16	5
portend	Port Number to End	uint16	5

## 22016 - LOG\_ID\_IPPOOLPBA\_DEALLOCATE

**Message ID:** 22016

**Message Description:** LOG\_ID\_IPPOOLPBA\_DEALLOCATE

**Message Meaning:** Deallocate IP pool PBA

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
nat	NAT IP Address	ip	39
saddr	Source Address IP	string	80
poolname	IP Pool Name	string	36
portbegin	Port Number to Begin	uint16	5
portend	Port Number to End	uint16	5
duration	Duration	uint32	10

## 22017 - LOG\_ID\_EXCEED\_GLOB\_RES\_LIMIT

**Message ID:** 22017

**Message Description:** LOG\_ID\_EXCEED\_GLOB\_RES\_LIMIT

**Message Meaning:** Global resource limit exceeded

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
service	Name of Service	string	64

## 22018 - LOG\_ID\_EXCEED\_VD\_RES\_LIMIT

**Message ID:** 22018

**Message Description:** LOG\_ID\_EXCEED\_VD\_RES\_LIMIT

**Message Meaning:** VDOM resource limit exceeded

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
service	Name of Service	string	64

## 22019 - LOG\_ID\_LOGRATE\_OVER\_LIMIT

**Message ID:** 22019

**Message Description:** LOG\_ID\_LOGRATE\_OVER\_LIMIT

**Message Meaning:** Log rate limit exceeded

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22020 - LOG\_ID\_FAIL\_CREATE\_HA\_SOCKET

**Message ID:** 22020**Message Description:** LOG\_ID\_FAIL\_CREATE\_HA\_SOCKET**Message Meaning:** HA socket creation failed**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22021 - LOG\_ID\_FAIL\_CREATE\_HA\_SOCKET\_RETRY

**Message ID:** 22021

**Message Description:** LOG\_ID\_FAIL\_CREATE\_HA\_SOCKET\_RETRY

**Message Meaning:** UDP socket creation to relay URL request failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22031 - LOG\_ID\_SUCCESS\_CSF\_LOG\_SYNC\_CONFIG\_CHANGED

**Message ID:** 22031

**Message Description:** LOG\_ID\_SUCCESS\_CSF\_LOG\_SYNC\_CONFIG\_CHANGED

**Message Meaning:** Settings modified by Security Fabric service

**Type:** Event

**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
sn	Serial Number	string	64

## 22032 - LOG\_ID\_CSF\_LOOP\_FOUND

**Message ID:** 22032**Message Description:** LOG\_ID\_CSF\_LOOP\_FOUND**Message Meaning:** Looped configuration in Security Fabric service**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256
sn	Serial Number	string	64
path		string	512

## 22035 - LOG\_ID\_CSF\_UPSTREAM\_SN\_CHANGED

**Message ID:** 22035

**Message Description:** LOG\_ID\_CSF\_UPSTREAM\_SN\_CHANGED

**Message Meaning:** Serial number of upstream is changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5



Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
ip		ip	39
oldsn	Security fabric upstream FGT old serial number	string	64

## 22036 - LOG\_ID\_CSF\_FGT\_CONNECTED

**Message ID:** 22036

**Message Description:** LOG\_ID\_CSF\_FGT\_CONNECTED

**Message Meaning:** Connection with CSF member established and authorized

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
ip		ip	39
direction		string	16

## 22037 - LOG\_ID\_CSF\_FGT\_DISCONNECTED

**Message ID:** 22037

**Message Description:** LOG\_ID\_CSF\_FGT\_DISCONNECTED

**Message Meaning:** Connection with authorized CSF member terminated

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
reason	Reason	string	256
sn	Serial Number	string	64
ip		ip	39
direction		string	16

## 22038 - LOG\_ID\_CSF\_GLOBAL\_SYNC\_FAILED

**Message ID:** 22038

**Message Description:** LOG\_ID\_CSF\_GLOBAL\_SYNC\_FAILED

**Message Meaning:** Synchronization of global object failed.

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256
sn	Serial Number	string	64
path		string	512

## 22039 - LOG\_ID\_CSF\_GLOBAL\_SYNC\_REPORT

**Message ID:** 22039

**Message Description:** LOG\_ID\_CSF\_GLOBAL\_SYNC\_REPORT

**Message Meaning:** Synchronization of global object report.

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256
sn	Serial Number	string	64
path		string	512
cmdbpathname		string	96
cmdbtablename		string	64
errorcount		int32	10
conflictcount		int32	10
successcount		int32	10

## 22050 - LOG\_ID\_IPAMD\_ADDRESS\_ALLOCATED

**Message ID:** 22050

**Message Description:** LOG\_ID\_IPAMD\_ADDRESS\_ALLOCATED

**Message Meaning:** Address allocated by FortiIPAM and applied to an interface

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
ip		ip	39
interface	Interface	string	32

## 22051 - LOG\_ID\_IPAMD\_ADDRESS\_SET\_FAILED

**Message ID:** 22051

**Message Description:** LOG\_ID\_IPAMD\_ADDRESS\_SET\_FAILED

**Message Meaning:** Address received from FortiIPAM could not be applied to the interface

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
ip		ip	39
interface	Interface	string	32

## 22052 - LOG\_ID\_IPAMD\_ADDRESS\_INVALIDATED

**Message ID:** 22052

**Message Description:** LOG\_ID\_IPAMD\_ADDRESS\_INVALIDATED

**Message Meaning:** FortiIPAM indicated that the address was no longer allocated to the interface

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
interface	Interface	string	32

## 22053 - LOG\_ID\_IPAMD\_VALIDATION\_COMPLETE

**Message ID:** 22053

**Message Description:** LOG\_ID\_IPAMD\_VALIDATION\_COMPLETE

**Message Meaning:** Startup validation of IPAM addresses was completed

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22100 - LOG\_ID\_QUAR\_DROP\_TRAN\_JOB

**Message ID:** 22100**Message Description:** LOG\_ID\_QUAR\_DROP\_TRAN\_JOB**Message Meaning:** Files dropped by quarantine daemon**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
count	Count	uint32	10
limit	Virtual Domain Resource Limit	uint32	10
reason	Reason	string	256
used	Number of Used IPs	uint32	10
duration	Duration	uint32	10
fams_pause	Fortinet Analysis and Management Service Pause	uint32	10

## 22101 - LOG\_ID\_QUAR\_DROP\_TLL\_JOB

**Message ID:** 22101

**Message Description:** LOG\_ID\_QUAR\_DROP\_TLL\_JOB

**Message Meaning:** Files dropped due to poor network connection

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20



Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
count	Count	uint32	10
reason	Reason	string	256

## 22102 - LOG\_ID\_LOG\_DISK\_FAILURE

**Message ID:** 22102

**Message Description:** LOG\_ID\_LOG\_DISK\_FAILURE

**Message Meaning:** Log disk failure imminent

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22103 - LOG\_ID\_QUAR\_LIMIT\_REACHED

**Message ID:** 22103

**Message Description:** LOG\_ID\_QUAR\_LIMIT\_REACHED**Message Meaning:** Sandbox limit reached**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
count	Count	uint32	10
limit	Virtual Domain Resource Limit	uint32	10

## 22104 - LOG\_ID\_POWER\_RESTORE

**Message ID:** 22104**Message Description:** LOG\_ID\_POWER\_RESTORE**Message Meaning:** Power supply restored**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
unit	Unit	uint32	10

## 22105 - LOG\_ID\_POWER\_FAILURE

**Message ID:** 22105

**Message Description:** LOG\_ID\_POWER\_FAILURE

**Message Meaning:** Power supply failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
unit	Unit	uint32	10

## 22106 - LOG\_ID\_POWER\_OPTIONAL\_NOT\_DETECTED

**Message ID:** 22106

**Message Description:** LOG\_ID\_POWER\_OPTIONAL\_NOT\_DETECTED

**Message Meaning:** Optional power supply not detected

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22107 - LOG\_ID\_VOLT\_ANOM

**Message ID:** 22107

**Message Description:** LOG\_ID\_VOLT\_ANOM

**Message Meaning:** Voltage anomaly

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22108 - LOG\_ID\_FAN\_ANOM

**Message ID:** 22108

**Message Description:** LOG\_ID\_FAN\_ANOM

**Message Meaning:** Fan anomaly

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22109 - LOG\_ID\_TEMP\_TOO\_HIGH

**Message ID:** 22109

**Message Description:** LOG\_ID\_TEMP\_TOO\_HIGH

**Message Meaning:** Temperature too high

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22110 - LOG\_ID\_SPARE\_BLOCK\_LOW

**Message ID:** 22110

**Message Description:** LOG\_ID\_SPARE\_BLOCK\_LOW

**Message Meaning:** Spare blocks availability low

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22113 - LOG\_ID\_FNBAM\_FAILURE

**Message ID:** 22113

**Message Description:** LOG\_ID\_FNBAM\_FAILURE**Message Meaning:** Authentication error**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
service	Name of Service	string	64

## 22114 - LOG\_ID\_POWER\_REDUNDANCY\_DEGRADE

**Message ID:** 22114**Message Description:** LOG\_ID\_POWER\_REDUNDANCY\_DEGRADE**Message Meaning:** Power Supply Redundancy Degrade**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10



Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22115 - LOG\_ID\_POWER\_REDUNDANCY\_FAILURE

**Message ID:** 22115

**Message Description:** LOG\_ID\_POWER\_REDUNDANCY\_FAILURE

**Message Meaning:** Power Supply Redundancy Lost

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22150 - LOG\_ID\_VOLT\_NOM

**Message ID:** 22150

**Message Description:** LOG\_ID\_VOLT\_NOM

**Message Meaning:** Voltage normal

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22151 - LOG\_ID\_FAN\_NOM

**Message ID:** 22151

**Message Description:** LOG\_ID\_FAN\_NOM

**Message Meaning:** Fan normal

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22152 - LOG\_ID\_TEMP\_TOO\_LOW

**Message ID:** 22152

**Message Description:** LOG\_ID\_TEMP\_TOO\_LOW

**Message Meaning:** Temperature too low

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22153 - LOG\_ID\_TEMP\_NORM

**Message ID:** 22153

**Message Description:** LOG\_ID\_TEMP\_NORM

**Message Meaning:** Temperature normal

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22200 - LOG\_ID\_AUTO\_UPT\_CERT

**Message ID:** 22200

**Message Description:** LOG\_ID\_AUTO\_UPT\_CERT

**Message Meaning:** Certificate will be auto-updated

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
cert	Certificate	string	36

## 22201 - LOG\_ID\_AUTO\_GEN\_CERT

**Message ID:** 22201

**Message Description:** LOG\_ID\_AUTO\_GEN\_CERT

**Message Meaning:** Certificate will be auto-regenerated

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
cert	Certificate	string	36

## 22203 - LOG\_ID\_AUTO\_GEN\_CERT\_FAIL

**Message ID:** 22203

**Message Description:** LOG\_ID\_AUTO\_GEN\_CERT\_FAIL

**Message Meaning:** Certificate failed to auto-generate

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
name	Display Name of the Connection	string	128

## 22204 - LOG\_ID\_AUTO\_GEN\_CERT\_PENDING

**Message ID:** 22204

**Message Description:** LOG\_ID\_AUTO\_GEN\_CERT\_PENDING

**Message Meaning:** Certificate pending to auto-generate

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
name	Display Name of the Connection	string	128

## 22205 - LOG\_ID\_AUTO\_GEN\_CERT\_SUCC

**Message ID:** 22205

**Message Description:** LOG\_ID\_AUTO\_GEN\_CERT\_SUCC

**Message Meaning:** Certificate succeed to auto-generate

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5



Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
name	Display Name of the Connection	string	128

## 22206 - LOG\_ID\_CRL\_EXPIRED

**Message ID:** 22206

**Message Description:** LOG\_ID\_CRL\_EXPIRED

**Message Meaning:** CRL is expired

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22220 - LOG\_ID\_EXT\_RESOURCE

**Message ID:** 22220

**Message Description:** LOG\_ID\_EXT\_RESOURCE

**Message Meaning:** Threat feed updated

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
desc	Description	string	128

## 22221 - LOG\_ID\_EXT\_RESOURCE\_FAIL

**Message ID:** 22221

**Message Description:** LOG\_ID\_EXT\_RESOURCE\_FAIL

**Message Meaning:** Threat feed update failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256
desc	Description	string	128

## 22222 - LOG\_ID\_EXT\_RESOURCE\_LOAD

**Message ID:** 22222

**Message Description:** LOG\_ID\_EXT\_RESOURCE\_LOAD

**Message Meaning:** Threat feed loaded

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
file	Report file full path	string	256
filesize	Report File Size in Bytes	uint32	10
reason	Reason	string	256
desc	Description	string	128
created		string	64
informationsource	Information Source	string	4096
new_status	New Status	string	512

## 22223 - LOG\_ID\_EXT\_RESOURCE\_DEBUG

**Message ID:** 22223

**Message Description:** LOG\_ID\_EXT\_RESOURCE\_DEBUG

**Message Meaning:** Threat feed debug

**Type:** Event

**Category:** SYSTEM

**Severity:** Debug

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
dstport	Destination Protocol Port	uint16	5
path		string	512
desc	Description	string	128
informationsource	Information Source	string	4096
profile	Profile Name	string	64
hostname	Hostname	string	128
host		string	256
old_status	Original Status	string	512

## 22700 - LOG\_ID\_IPS\_FAIL\_OPEN

**Message ID:** 22700

**Message Description:** LOG\_ID\_IPS\_FAIL\_OPEN

**Message Meaning:** IPS session scan paused

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 22701 - LOG\_ID\_IPS\_FAIL\_OPEN\_END

**Message ID:** 22701

**Message Description:** LOG\_ID\_IPS\_FAIL\_OPEN\_END

**Message Meaning:** IPS session scan resumed

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22800 - LOG\_ID\_SCAN\_SERV\_FAIL

**Message ID:** 22800

**Message Description:** LOG\_ID\_SCAN\_SERV\_FAIL

**Message Meaning:** Scan services session failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
service	Name of Service	string	64
mode	Mode	string	12

## 22802 - LOG\_ID\_ENTER\_FD\_CONSERVE\_MODE

**Message ID:** 22802

**Message Description:** LOG\_ID\_ENTER\_FD\_CONSERVE\_MODE

**Message Meaning:** File descriptor conserve mode entered

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
daemon	Daemon Name	string	32
conserve	Flag for Conserve Mode	string	32
total	Total	uint32	10
used	Number of Used IPs	uint32	10
red		string	32
green	Green threshold for conserve mode	string	32

## 22803 - LOG\_ID\_LEAVE\_FD\_CONSERVE\_MODE

**Message ID:** 22803

**Message Description:** LOG\_ID\_LEAVE\_FD\_CONSERVE\_MODE

**Message Meaning:** File descriptor conserve mode exited

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11



Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
daemon	Daemon Name	string	32
conserve	Flag for Conserve Mode	string	32
total	Total	uint32	10
used	Number of Used IPs	uint32	10
red		string	32
green	Green threshold for conserve mode	string	32

## 22804 - LOG\_ID\_LIC\_STATUS\_CHG

**Message ID:** 22804

**Message Description:** LOG\_ID\_LIC\_STATUS\_CHG

**Message Meaning:** License status changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
service	Name of Service	string	64
sn	Serial Number	string	64

## 22805 - LOG\_ID\_FAIL\_TO\_VALIDATE\_LIC

**Message ID:** 22805

**Message Description:** LOG\_ID\_FAIL\_TO\_VALIDATE\_LIC

**Message Meaning:** License validation failure

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
service	Name of Service	string	64
sn	Serial Number	string	64

## 22806 - LOG\_ID\_DUP\_LIC

**Message ID:** 22806

**Message Description:** LOG\_ID\_DUP\_LIC

**Message Meaning:** Duplicate license detected

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
service	Name of Service	string	64
sn	Serial Number	string	64

## 22807 - LOG\_ID\_VDOM\_LIC

**Message ID:** 22807

**Message Description:** LOG\_ID\_VDOM\_LIC

**Message Meaning:** VDOM license status changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
service	Name of Service	string	64
sn	Serial Number	string	64

## 22808 - LOG\_ID\_LIC\_EXPIRE

**Message ID:** 22808

**Message Description:** LOG\_ID\_LIC\_EXPIRE

**Message Meaning:** VM license expired

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
service	Name of Service	string	64
sn	Serial Number	string	64

## 22809 - LOG\_ID\_LIC\_WILL\_EXPIRE

**Message ID:** 22809

**Message Description:** LOG\_ID\_LIC\_WILL\_EXPIRE

**Message Meaning:** VM license expiring

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
service	Name of Service	string	64
sn	Serial Number	string	64

## 22810 - LOG\_ID\_SCANUNIT\_ERROR\_BLOCK

**Message ID:** 22810

**Message Description:** LOG\_ID\_SCANUNIT\_ERROR\_BLOCK

**Message Meaning:** Scan error - traffic blocked

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
service	Name of Service	string	64
proto	Protocol Number	uint8	3
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5

Log Field Name	Description	Data Type	Length
file	Report file full path	string	256
session_id	Session ID	uint32	10
src_int	Source Interface	string	64
dst_int	Destination Interface	string	64
dir	Direction	string	8

## 22811 - LOG\_ID\_SCANUNIT\_ERROR\_PASS

**Message ID:** 22811

**Message Description:** LOG\_ID\_SCANUNIT\_ERROR\_PASS

**Message Meaning:** Scan error - traffic passed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
service	Name of Service	string	64
proto	Protocol Number	uint8	3
srcip	Source IP	ip	39
srcport	Source port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
file	Report file full path	string	256
session_id	Session ID	uint32	10
src_int	Source Interface	string	64
dst_int	Destination Interface	string	64
dir	Direction	string	8

## 22812 - LOG\_ID\_SCANUNIT\_AVENG\_RELOAD

**Message ID:** 22812

**Message Description:** LOG\_ID\_SCANUNIT\_AVENG\_RELOAD

**Message Meaning:** Scanunit is reloading AV engine

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096



## 22813 - LOG\_ID\_SCANUNIT\_AVDB\_RELOAD

**Message ID:** 22813

**Message Description:** LOG\_ID\_SCANUNIT\_AVDB\_RELOAD

**Message Meaning:** Scanunit reloaded AV Database

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 22814 - LOG\_ID\_SCANUNIT\_AVDB\_RELOAD\_ERROR

**Message ID:** 22814

**Message Description:** LOG\_ID\_SCANUNIT\_AVDB\_RELOAD\_ERROR

**Message Meaning:** Scanunit AV Database reload error

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 22815 - LOG\_ID\_SCANUNIT\_AVDB\_LOAD

**Message ID:** 22815

**Message Description:** LOG\_ID\_SCANUNIT\_AVDB\_LOAD

**Message Meaning:** Scanunit loaded AV Database

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 22816 - LOG\_ID\_SCANUNIT\_AVDB\_LOAD\_ERROR

**Message ID:** 22816

**Message Description:** LOG\_ID\_SCANUNIT\_AVDB\_LOAD\_ERROR

**Message Meaning:** Scanunit AV Database load error

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 22850 - LOG\_ID\_USER\_QUARANTINE\_MAC\_ADD

**Message ID:** 22850

**Message Description:** LOG\_ID\_USER\_QUARANTINE\_MAC\_ADD

**Message Meaning:** User quarantine MAC added

**Type:** Event**Category:** SWITCH-CONTROLLER**Severity:** Notice

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
action		string	65
msg		string	4096

## 22851 - LOG\_ID\_USER\_QUARANTINE\_MAC\_DELETE

**Message ID:** 22851**Message Description:** LOG\_ID\_USER\_QUARANTINE\_MAC\_DELETE**Message Meaning:** User quarantine MAC deleted**Type:** Event**Category:** SWITCH-CONTROLLER**Severity:** Notice

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10

Log Field Name	Description	Data Type	Length
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
action		string	65
msg		string	4096

## 22852 - LOG\_ID\_USER\_QUARANTINE\_MAC\_BOUNCE\_PORT\_HIT

**Message ID:** 22852

**Message Description:** LOG\_ID\_USER\_QUARANTINE\_MAC\_BOUNCE\_PORT\_HIT

**Message Meaning:** User quarantine MAC bounce port hit

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20

Log Field Name	Description	Data Type	Length
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
action		string	65
msg		string	4096
sn		string	64
name		string	128

## 22853 - LOG\_ID\_USER\_QUARANTINE\_MAC\_BOUNCE\_PORT\_MISS

**Message ID:** 22853

**Message Description:** LOG\_ID\_USER\_QUARANTINE\_MAC\_BOUNCE\_PORT\_MISS

**Message Meaning:** User quarantine MAC bounce port miss

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64

Log Field Name	Description	Data Type	Length
action		string	65
msg		string	4096
sn		string	64
name		string	128

## 22890 - LOG\_ID\_FORTILINKD

**Message ID:** 22890

**Message Description:** LOG\_ID\_FORTILINKD

**Message Meaning:** Switch-Controller Daemon Log (Notification)

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 22891 - LOG\_ID\_FLCFGD\_SYNC\_ERROR

**Message ID:** 22891

**Message Description:** LOG\_ID\_FLCFGD\_SYNC\_ERROR

**Message Meaning:** Switch-Controller Switch Sync Error

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Error

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 22892 - LOG\_ID\_FLCFGD\_SYNC\_COMPLETE

**Message ID:** 22892

**Message Description:** LOG\_ID\_FLCFGD\_SYNC\_COMPLETE

**Message Meaning:** Switch-Controller Switch Sync Complete

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information



Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 22893 - LOG\_ID\_FLCFGD\_SYNC\_STATE

**Message ID:** 22893

**Message Description:** LOG\_ID\_FLCFGD\_SYNC\_STATE

**Message Meaning:** Switch-Controller Switch Sync State

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Debug

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20

Log Field Name	Description	Data Type	Length
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 22894 - LOG\_ID\_FLCFGD\_UPGRADE\_ERROR

**Message ID:** 22894

**Message Description:** LOG\_ID\_FLCFGD\_UPGRADE\_ERROR

**Message Meaning:** Switch-Controller Switch Upgrade Error

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Error

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5

Log Field Name	Description	Data Type	Length
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 22895 - LOG\_ID\_FLCFGD\_UPGRADE\_STATUS

**Message ID:** 22895

**Message Description:** LOG\_ID\_FLCFGD\_UPGRADE\_STATUS

**Message Meaning:** Switch-Controller Switch Upgrade Status

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 22896 - LOG\_ID\_FORTILINKD\_CRITICAL

**Message ID:** 22896

**Message Description:** LOG\_ID\_FORTILINKD\_CRITICAL

**Message Meaning:** Switch-Controller Daemon Log (Critical)

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 22897 - LOG\_ID\_FLCFGD\_NAC\_ADD

**Message ID:** 22897

**Message Description:** LOG\_ID\_FLCFGD\_NAC\_ADD

**Message Meaning:** NAC device addition

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
action		string	65
msg		string	4096
sn		string	64
name		string	128

## 22898 - LOG\_ID\_FLCFGD\_NAC\_DELETE

**Message ID:** 22898

**Message Description:** LOG\_ID\_FLCFGD\_NAC\_DELETE

**Message Meaning:** NAC device deletion

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16

Log Field Name	Description	Data Type	Length
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
action		string	65
msg		string	4096
sn		string	64
name		string	128

## 22899 - LOG\_ID\_FLCFGD\_NAC\_MODIFY

**Message ID:** 22899

**Message Description:** LOG\_ID\_FLCFGD\_NAC\_MODIFY

**Message Meaning:** NAC device modify

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32

Log Field Name	Description	Data Type	Length
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
action		string	65
msg		string	4096
sn		string	64
name		string	128

## 22900 - LOG\_ID\_CAPUTP\_SESSION

**Message ID:** 22900

**Message Description:** LOG\_ID\_CAPUTP\_SESSION

**Message Meaning:** CAPUTP session status

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
msg		string	4096

## 22901 - LOG\_ID\_FAZ\_CON

**Message ID:** 22901

**Message Description:** LOG\_ID\_FAZ\_CON

**Message Meaning:** FortiAnalyzer connection up

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 22902 - LOG\_ID\_FAZ\_DISCON

**Message ID:** 22902

**Message Description:** LOG\_ID\_FAZ\_DISCON

**Message Meaning:** FortiAnalyzer connection down

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice



Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256

## 22903 - LOG\_ID\_FAZ\_CON\_ERR

**Message ID:** 22903

**Message Description:** LOG\_ID\_FAZ\_CON\_ERR

**Message Meaning:** FortiAnalyzer connection failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256

## 22904 - LOG\_ID\_CAPUTP\_SESSION\_NOTIF

**Message ID:** 22904

**Message Description:** LOG\_ID\_CAPUTP\_SESSION\_NOTIF

**Message Meaning:** CAPUTP session status notification

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256

Log Field Name	Description	Data Type	Length
ui		string	64
action		string	65
msg		string	4096
sn		string	64
name		string	128
srcip		ip	39

## 22912 - LOG\_ID\_FDS\_SRV\_ERRCON

**Message ID:** 22912

**Message Description:** LOG\_ID\_FDS\_SRV\_ERRCON

**Message Meaning:** FortiCloud server connection failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
server	Server IP Address	string	64
reason	Reason	string	256

## 22913 - LOG\_ID\_FDS\_SRV\_DISCON

**Message ID:** 22913

**Message Description:** LOG\_ID\_FDS\_SRV\_DISCON

**Message Meaning:** FortiCloud server disconnected

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
server	Server IP Address	string	64
reason	Reason	string	256

## 22914 - LOG\_ID\_FDS\_SRV\_CHG

**Message ID:** 22914

**Message Description:** LOG\_ID\_FDS\_SRV\_CHG

**Message Meaning:** FortiCloud server changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
server	Server IP Address	string	64

## 22915 - LOG\_ID\_FDS\_SRV\_CON

**Message ID:** 22915

**Message Description:** LOG\_ID\_FDS\_SRV\_CON

**Message Meaning:** FortiCloud server connected

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
server	Server IP Address	string	64

## 22916 - LOG\_ID\_FDS\_STATUS

**Message ID:** 22916

**Message Description:** LOG\_ID\_FDS\_STATUS

**Message Meaning:** FortiGuard Message Service status

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096

## 22917 - LOG\_ID\_FDS\_SMS\_QUOTA

**Message ID:** 22917

**Message Description:** LOG\_ID\_FDS\_SMS\_QUOTA

**Message Meaning:** SMS quota reached

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
msg	Log Message	string	4096

## 22918 - LOG\_ID\_FDS\_CTRL\_STATUS

**Message ID:** 22918

**Message Description:** LOG\_ID\_FDS\_CTRL\_STATUS

**Message Meaning:** FortiGuard Message Service controller status

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096

## 22919 - LOG\_ID\_SVR\_LOG\_STATUS\_CHANGED

**Message ID:** 22919

**Message Description:** LOG\_ID\_SVR\_LOG\_STATUS\_CHANGED

**Message Meaning:** Server logging status changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20



Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22921 - LOG\_ID\_EVENT\_ROUTE\_INFO\_CHANGED

**Message ID:** 22921

**Message Description:** LOG\_ID\_EVENT\_ROUTE\_INFO\_CHANGED

**Message Meaning:** Routing information changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
name	Display Name of the Connection	string	128
interface	Interface	string	32

## 22922 - LOG\_ID\_EVENT\_LINK\_MONITOR\_STATUS

**Message ID:** 22922

**Message Description:** LOG\_ID\_EVENT\_LINK\_MONITOR\_STATUS

**Message Meaning:** Link monitor status

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
name	Display Name of the Connection	string	128
interface	Interface	string	32
probeprotocol	Link Monitor Probe Protocol	string	16

## 22923 - LOG\_ID\_EVENT\_VWL\_LQTY\_STATUS

**Message ID:** 22923

**Message Description:** LOG\_ID\_EVENT\_VWL\_LQTY\_STATUS

**Message Meaning:** Virtual WAN Link status

**Type:** Event

**Category:** SDWAN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
eventtype		string	32
serviceid		uint32	10
service	Name of Service	string	64
healthcheck		string	64
slatargetid		uint32	10
member		string	512
numpassmember		uint32	10
oldvalue		string	32
newvalue		string	32
interface	Interface	string	32
msg	Log Message	string	4096

## 22924 - LOG\_ID\_EVENT\_VWL\_VOLUME\_STATUS

**Message ID:** 22924

**Message Description:** LOG\_ID\_EVENT\_VWL\_VOLUME\_STATUS

**Message Meaning:** Virtual WAN Link volume status

**Type:** Event

**Category:** SDWAN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
eventtype		string	32
member		string	512
interface	Interface	string	32
msg	Log Message	string	4096

## 22925 - LOG\_ID\_EVENT\_VWL\_SLA\_INFO

**Message ID:** 22925

**Message Description:** LOG\_ID\_EVENT\_VWL\_SLA\_INFO

**Message Meaning:** Virtual WAN Link SLA information

**Type:** Event

**Category:** SDWAN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
eventtype		string	32
healthcheck		string	64
oldvalue		string	32
newvalue		string	32
interface	Interface	string	32
msg	Log Message	string	4096
probeprotocol	Link Monitor Probe Protocol	string	16
status	Status	string	23
latency		string	24
jitter		string	24
packetloss		string	24
inbandwidth		string	24
outbandwidth		string	24
bandwidth		string	24
inbandwidthused		string	24
outbandwidthused		string	24
bandwidthused		string	24
slamap		string	24

## 22926 - LOG\_ID\_EVENT\_VWL\_NEIGHBOR\_STATUS

**Message ID:** 22926

**Message Description:** LOG\_ID\_EVENT\_VWL\_NEIGHBOR\_STATUS

**Message Meaning:** Virtual WAN Link Neighbor status

**Type:** Event

**Category:** SDWAN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
eventtype		string	32
member		string	512
msg	Log Message	string	4096
neighbor		string	46

## 22927 - LOG\_ID\_EVENT\_VWL\_NEIGHBOR\_STANDALONE

**Message ID:** 22927

**Message Description:** LOG\_ID\_EVENT\_VWL\_NEIGHBOR\_STANDALONE

**Message Meaning:** Virtual WAN Link Neighbor standalone

**Type:** Event

**Category:** SDWAN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
eventtype		string	32
oldvalue		string	32
newvalue		string	32
msg	Log Message	string	4096

## 22928 - LOG\_ID\_EVENT\_VWL\_NEIGHBOR\_PRIMARY

**Message ID:** 22928

**Message Description:** LOG\_ID\_EVENT\_VWL\_NEIGHBOR\_PRIMARY

**Message Meaning:** Virtual WAN Link Neighbor primary

**Type:** Event

**Category:** SDWAN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
eventtype		string	32

Log Field Name	Description	Data Type	Length
oldvalue		string	32
newvalue		string	32
msg	Log Message	string	4096

## 22929 - LOG\_ID\_EVENT\_VWL\_NEIGHBOR\_SECONDARY

**Message ID:** 22929

**Message Description:** LOG\_ID\_EVENT\_VWL\_NEIGHBOR\_SECONDARY

**Message Meaning:** Virtual WAN Link Neighbor secondary

**Type:** Event

**Category:** SDWAN

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
eventtype		string	32
oldvalue		string	32
newvalue		string	32
msg	Log Message	string	4096

## 22949 - LOG\_ID\_FDS\_JOIN

**Message ID:** 22949

**Message Description:** LOG\_ID\_FDS\_JOIN



**Message Meaning:** FortiCloud auto-join attempted

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 22950 - LOG\_ID\_FDS\_LOGIN\_SUCC

**Message ID:** 22950

**Message Description:** LOG\_ID\_FDS\_LOGIN\_SUCC

**Message Meaning:** FortiCloud activation successful

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 22951 - LOG\_ID\_FDS\_LOGOUT

**Message ID:** 22951

**Message Description:** LOG\_ID\_FDS\_LOGOUT

**Message Meaning:** FortiCloud logout

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 22952 - LOG\_ID\_FDS\_LOGIN\_FAIL

**Message ID:** 22952

**Message Description:** LOG\_ID\_FDS\_LOGIN\_FAIL

**Message Meaning:** FortiCloud activation failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 22953 - LOG\_ID\_IOC\_DETECTED

**Message ID:** 22953

**Message Description:** LOG\_ID\_IOC\_DETECTED

**Message Meaning:** Compromised host detected

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 22954 - LOG\_ID\_INET\_SVC\_OBSOLETE

**Message ID:** 22954

**Message Description:** LOG\_ID\_INET\_SVC\_OBSOLETE

**Message Meaning:** Internet Service obsolete

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22955 - LOG\_ID\_INET\_SVC\_NAME\_FAILURE

**Message ID:** 22955

**Message Description:** LOG\_ID\_INET\_SVC\_NAME\_FAILURE

**Message Meaning:** Internet Service name update failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 22956 - LOG\_ID\_INET\_SVC\_NAME\_UPDATE

**Message ID:** 22956

**Message Description:** LOG\_ID\_INET\_SVC\_NAME\_UPDATE

**Message Meaning:** Internet Service name update

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 23101 - LOG\_ID\_IPSEC\_TUNNEL\_UP

**Message ID:** 23101

**Message Description:** LOG\_ID\_IPSEC\_TUNNEL\_UP

**Message Meaning:** IPsec VPN tunnel up

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
tunnelip	IPsec VPN tunnel IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096

## 23102 - LOG\_ID\_IPSEC\_TUNNEL\_DOWN

**Message ID:** 23102

**Message Description:** LOG\_ID\_IPSEC\_TUNNEL\_DOWN

**Message Meaning:** IPsec VPN tunnel down

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
tunnelip	IPsec VPN tunnel IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096

## 23103 - LOG\_ID\_IPSEC\_TUNNEL\_STAT

**Message ID:** 23103

**Message Description:** LOG\_ID\_IPSEC\_TUNNEL\_STAT

**Message Meaning:** IPsec VPN tunnel statistics

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20



Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
tunnelip	IPsec VPN tunnel IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096

## 26001 - LOG\_ID\_DHCP\_ACK

**Message ID:** 26001

**Message Description:** LOG\_ID\_DHCP\_ACK

**Message Meaning:** DHCP Ack log

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ip		ip	39
interface	Interface	string	32
hostname	Hostname	string	128
dhcp_msg	DHCP Message	string	4096
mac	MAC Address	string	17
lease	DHCP lease time	uint32	10

## 26002 - LOG\_ID\_DHCP\_RELEASE

**Message ID:** 26002

**Message Description:** LOG\_ID\_DHCP\_RELEASE

**Message Meaning:** DHCP Release log

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
ip		ip	39
interface	Interface	string	32

Log Field Name	Description	Data Type	Length
hostname	Hostname	string	128
dhcp_msg	DHCP Message	string	4096
mac	MAC Address	string	17

## 26003 - LOG\_ID\_DHCP\_STAT

**Message ID:** 26003

**Message Description:** LOG\_ID\_DHCP\_STAT

**Message Meaning:** DHCP statistics

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
total	Total	uint32	10
used	Number of Used IPs	uint32	10
interface	Interface	string	32

## 26004 - LOG\_ID\_DHCP\_CLIENT\_LEASE

**Message ID:** 26004

**Message Description:** LOG\_ID\_DHCP\_CLIENT\_LEASE

**Message Meaning:** DHCP client lease granted

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 26005 - LOG\_ID\_DHCP\_LEASE\_USAGE\_HIGH

**Message ID:** 26005

**Message Description:** LOG\_ID\_DHCP\_LEASE\_USAGE\_HIGH

**Message Meaning:** DHCP lease usage high

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
interface	Interface	string	32

## 26006 - LOG\_ID\_DHCP\_LEASE\_USAGE\_FULL

**Message ID:** 26006

**Message Description:** LOG\_ID\_DHCP\_LEASE\_USAGE\_FULL

**Message Meaning:** DHCP lease usage full

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
interface	Interface	string	32

## 26007 - LOG\_ID\_DHCP\_BLOCKED\_MAC

**Message ID:** 26007

**Message Description:** LOG\_ID\_DHCP\_BLOCKED\_MAC

**Message Meaning:** DHCP client blocked log

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
interface	Interface	string	32
mac	MAC Address	string	17

## 26008 - LOG\_ID\_DHCP\_DDNS\_ADD

**Message ID:** 26008

**Message Description:** LOG\_ID\_DHCP\_DDNS\_ADD

**Message Meaning:** DHCP DDNS add query

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
ip		ip	39
dhcp_msg	DHCP Message	string	4096
ddnsserver	DDNS Server	ip	39
fqdn	Fully Qualified Domain Name	string	256

## 26009 - LOG\_ID\_DHCP\_DDNS\_DELETE

**Message ID:** 26009

**Message Description:** LOG\_ID\_DHCP\_DDNS\_DELETE

**Message Meaning:** DHCP DDNS delete query

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
ip		ip	39
dhcp_msg	DHCP Message	string	4096
ddnsserver	DDNS Server	ip	39
fqdn	Fully Qualified Domain Name	string	256

## 26010 - LOG\_ID\_DHCP\_DDNS\_COMPLETED

**Message ID:** 26010

**Message Description:** LOG\_ID\_DHCP\_DDNS\_COMPLETED

**Message Meaning:** DHCP DDNS query completed

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5



Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
msg	Log Message	string	4096
ip		ip	39
dhcp_msg	DHCP Message	string	4096
ddnsserver	DDNS Server	ip	39
fqdn	Fully Qualified Domain Name	string	256

## 26011 - LOG\_ID\_DHCPV6\_REPLY

**Message ID:** 26011

**Message Description:** LOG\_ID\_DHCPV6\_REPLY

**Message Meaning:** DHCPv6 Ack log

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
ip		ip	39
interface	Interface	string	32
dhcp_msg	DHCP Message	string	4096

Log Field Name	Description	Data Type	Length
lease	DHCP lease time	uint32	10
duid	DHCPv6 unique identifier	string	128
iaid	DHCPv6 Identity Association Identifier	uint32	10

## 26012 - LOG\_ID\_DHCPV6\_RELEASE

**Message ID:** 26012

**Message Description:** LOG\_ID\_DHCPV6\_RELEASE

**Message Meaning:** DHCPv6 Release log

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
ip		ip	39
interface	Interface	string	32
dhcp_msg	DHCP Message	string	4096
lease	DHCP lease time	uint32	10
duid	DHCPv6 unique identifier	string	128
iaid	DHCPv6 Identity Association Identifier	uint32	10

## 27001 - LOG\_ID\_VRRP\_STATE\_CHG

**Message ID:** 27001

**Message Description:** LOG\_ID\_VRRP\_STATE\_CHG

**Message Meaning:** VRRP state changed

**Type:** Event

**Category:** ROUTER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
interface	Interface	string	32

## 29001 - LOG\_ID\_PPPD\_MSG

**Message ID:** 29001

**Message Description:** LOG\_ID\_PPPD\_MSG

**Message Meaning:** PPP status

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
status	Status	string	23
msg	Log Message	string	4096
local	Local IP for a PPPD Connection	ip	39
remote	IP Address of the PPP Remote end	ip	39
assigned	Assigned IP Address through PPPoE	ip	39

## 29002 - LOG\_ID\_PPPD\_AUTH\_SUC

**Message ID:** 29002

**Message Description:** LOG\_ID\_PPPD\_AUTH\_SUC

**Message Meaning:** PPP authentication successful

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096
local	Local IP for a PPPD Connection	ip	39
remote	IP Address of the PPP Remote end	ip	39
assigned	Assigned IP Address through PPPoE	ip	39

## 29003 - LOG\_ID\_PPPD\_AUTH\_FAIL

**Message ID:** 29003

**Message Description:** LOG\_ID\_PPPD\_AUTH\_FAIL

**Message Meaning:** PPP authentication failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
local	Local IP for a PPPD Connection	ip	39
remote	IP Address of the PPP Remote end	ip	39
assigned	Assigned IP Address through PPPoE	ip	39

## 29010 - LOG\_ID\_PPPOE\_STATUS\_REPORT\_NOTIF

**Message ID:** 29010

**Message Description:** LOG\_ID\_PPPOE\_STATUS\_REPORT\_NOTIF

**Message Meaning:** PPPoE status report

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
assigned	Assigned IP Address through PPPoE	ip	39
gateway	Gateway ip address for PPPoE status report	ip	39
mtu	Max Transmission Unit Value	uint32	10

## 29011 - LOG\_ID\_PPPD\_FAIL\_TO\_EXEC

**Message ID:** 29011

**Message Description:** LOG\_ID\_PPPD\_FAIL\_TO\_EXEC

**Message Meaning:** PPP execution failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 29012 - LOG\_ID\_PPP\_OPT\_ERR

**Message ID:** 29012

**Message Description:** LOG\_ID\_PPP\_OPT\_ERR

**Message Meaning:** PPP received incorrect options

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 29013 - LOG\_ID\_PPPD\_START

**Message ID:** 29013

**Message Description:** LOG\_ID\_PPPD\_START

**Message Meaning:** PPP daemon started

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096



## 29014 - LOG\_ID\_PPPD\_EXIT

**Message ID:** 29014

**Message Description:** LOG\_ID\_PPPD\_EXIT

**Message Meaning:** PPP daemon exited

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 29015 - LOG\_ID\_PPP\_RCV\_BAD\_PEER\_IP

**Message ID:** 29015

**Message Description:** LOG\_ID\_PPP\_RCV\_BAD\_PEER\_IP

**Message Meaning:** PPP received invalid peer IP

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 29016 - LOG\_ID\_PPP\_RCV\_BAD\_LOCAL\_IP

**Message ID:** 29016

**Message Description:** LOG\_ID\_PPP\_RCV\_BAD\_LOCAL\_IP

**Message Meaning:** PPP received invalid local IP

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 29017 - LOG\_ID\_PPP\_OPT\_NOTIF

**Message ID:** 29017

**Message Description:** LOG\_ID\_PPP\_OPT\_NOTIF

**Message Meaning:** PPP received incorrect notifications

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 29021 - LOG\_ID\_EVENT\_AUTH\_SNMP\_QUERY\_FAILED

**Message ID:** 29021

**Message Description:** LOG\_ID\_EVENT\_AUTH\_SNMP\_QUERY\_FAILED

**Message Meaning:** SNMP query failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
msg	Log Message	string	4096
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
community	Community	string	36
version	Version	string	64

## 29022 - LOG\_ID\_DDNS\_UPDATE\_FAIL

**Message ID:** 29022

**Message Description:** LOG\_ID\_DDNS\_UPDATE\_FAIL

**Message Meaning:** DDNS update failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32001 - LOG\_ID\_ADMIN\_LOGIN\_SUCC

**Message ID:** 32001

**Message Description:** LOG\_ID\_ADMIN\_LOGIN\_SUCC

**Message Meaning:** Admin login successful

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
dstip	Destination IP	ip	39
name	Display Name of the Connection	string	128
reason	Reason	string	256
sn	Serial number for login or logout events. Used to correlate login and logout events.	string	64
profile	Profile Name	string	64
method	Method	string	64

## 32002 - LOG\_ID\_ADMIN\_LOGIN\_FAIL

**Message ID:** 32002

**Message Description:** LOG\_ID\_ADMIN\_LOGIN\_FAIL

**Message Meaning:** Admin login failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
dstip	Destination IP	ip	39
name	Display Name of the Connection	string	128
reason	Reason	string	256
sn	Serial number for login or logout events. Used to correlate login and logout events.	string	64
method	Method	string	64

## 32003 - LOG\_ID\_ADMIN\_LOGOUT

**Message ID:** 32003

**Message Description:** LOG\_ID\_ADMIN\_LOGOUT

**Message Meaning:** Admin logout successful

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
dstip	Destination IP	ip	39
name	Display Name of the Connection	string	128
reason	Reason	string	256
duration	Duration	uint32	10
sn	Serial number for login or logout events. Used to correlate login and logout events.	string	64
method	Method	string	64
state	State	string	64

## 32005 - LOG\_ID\_ADMIN\_OVERRIDE\_VDOM

**Message ID:** 32005

**Message Description:** LOG\_ID\_ADMIN\_OVERRIDE\_VDOM

**Message Meaning:** Admin overrode VDOM

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32



Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256

## 32006 - LOG\_ID\_ADMIN\_ENTER\_VDOM

**Message ID:** 32006

**Message Description:** LOG\_ID\_ADMIN\_ENTER\_VDOM

**Message Meaning:** Super admin entered VDOM

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
msg	Log Message	string	4096
reason	Reason	string	256

## 32007 - LOG\_ID\_ADMIN\_LEFT\_VDOM

**Message ID:** 32007

**Message Description:** LOG\_ID\_ADMIN\_LEFT\_VDOM

**Message Meaning:** Super admin left VDOM

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
reason	Reason	string	256

## 32008 - LOG\_ID\_VIEW\_DISK\_LOG\_FAIL

**Message ID:** 32008

**Message Description:** LOG\_ID\_VIEW\_DISK\_LOG\_FAIL**Message Meaning:** Disk log access failed**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 32009 - LOG\_ID\_SYSTEM\_START

**Message ID:** 32009**Message Description:** LOG\_ID\_SYSTEM\_START**Message Meaning:** FortiGate started**Type:** Event**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32010 - LOG\_ID\_DISK\_LOG\_FULL

**Message ID:** 32010

**Message Description:** LOG\_ID\_DISK\_LOG\_FULL

**Message Meaning:** Disk full

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32011 - LOG\_ID\_LOG\_ROLL

**Message ID:** 32011

**Message Description:** LOG\_ID\_LOG\_ROLL

**Message Meaning:** Disk log rolled

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
reason	Reason	string	256
log	Log Name for Log Rotation	string	32

## 32014 - LOG\_ID\_CS\_LIC\_EXPIRE

**Message ID:** 32014

**Message Description:** LOG\_ID\_CS\_LIC\_EXPIRE

**Message Meaning:** Support license expiring

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32015 - LOG\_ID\_DISK\_LOG\_USAGE

**Message ID:** 32015

**Message Description:** LOG\_ID\_DISK\_LOG\_USAGE

**Message Meaning:** Log disk full

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32017 - LOG\_ID\_FDS\_DAILY\_QUOTA\_FULL

**Message ID:** 32017

**Message Description:** LOG\_ID\_FDS\_DAILY\_QUOTA\_FULL

**Message Meaning:** FortiCloud daily quota full

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32018 - LOG\_ID\_FIPS\_ENTER\_ERR\_MOD

**Message ID:** 32018

**Message Description:** LOG\_ID\_FIPS\_ENTER\_ERR\_MOD

**Message Meaning:** FIPS CC entered error mode

**Type:** Event

**Category:** SYSTEM

**Severity:** Emergency

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
reason	Reason	string	256

## 32019 - LOG\_ID\_CC\_ENTER\_ERR\_MOD

**Message ID:** 32019**Message Description:** LOG\_ID\_CC\_ENTER\_ERR\_MOD**Message Meaning:** CC entered error mode**Type:** Event**Category:** SYSTEM**Severity:** Emergency

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11



Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 32020 - LOG\_ID\_SSH\_CORRPUT\_MAC

**Message ID:** 32020

**Message Description:** LOG\_ID\_SSH\_CORRPUT\_MAC

**Message Meaning:** Message Authentication Code corrupted

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
ui	User Interface	string	64
msg	Log Message	string	4096

## 32021 - LOG\_ID\_ADMIN\_LOGIN\_DISABLE

**Message ID:** 32021

**Message Description:** LOG\_ID\_ADMIN\_LOGIN\_DISABLE

**Message Meaning:** Admin login disabled

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256

## 32022 - LOG\_ID\_VDOM\_ENABLED

**Message ID:** 32022

**Message Description:** LOG\_ID\_VDOM\_ENABLED

**Message Meaning:** VDOM enabled

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 32023 - LOG\_ID\_MEM\_LOG\_FIRST\_FULL

**Message ID:** 32023**Message Description:** LOG\_ID\_MEM\_LOG\_FIRST\_FULL**Message Meaning:** Memory log full over first warning level**Type:** Event**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32024 - LOG\_ID\_ADMIN\_PASSWD\_EXPIRE

**Message ID:** 32024

**Message Description:** LOG\_ID\_ADMIN\_PASSWD\_EXPIRE

**Message Meaning:** Admin password expired

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32025 - LOG\_ID\_SSH\_REKEY

**Message ID:** 32025

**Message Description:** LOG\_ID\_SSH\_REKEY

**Message Meaning:** SSH server re-key

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
ui	User Interface	string	64
msg	Log Message	string	4096

## 32026 - LOG\_ID\_SSH\_BAD\_PACKET\_LENGTH

**Message ID:** 32026

**Message Description:** LOG\_ID\_SSH\_BAD\_PACKET\_LENGTH

**Message Meaning:** SSH server received bad length packet

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
ui	User Interface	string	64
msg	Log Message	string	4096

## 32027 - LOG\_ID\_VIEW\_DISK\_LOG\_SUCC

**Message ID:** 32027

**Message Description:** LOG\_ID\_VIEW\_DISK\_LOG\_SUCC

**Message Meaning:** Disk logs viewed successfully

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 32028 - LOG\_ID\_LOG\_DEL\_DIR

**Message ID:** 32028

**Message Description:** LOG\_ID\_LOG\_DEL\_DIR

**Message Meaning:** Disk log directory deleted

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32029 - LOG\_ID\_LOG\_DEL\_FILE

**Message ID:** 32029

**Message Description:** LOG\_ID\_LOG\_DEL\_FILE

**Message Meaning:** Disk log file deleted

**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
filesize	Report File Size in Bytes	uint32	10

## 32030 - LOG\_ID\_SEND\_FDS\_STAT

**Message ID:** 32030**Message Description:** LOG\_ID\_SEND\_FDS\_STAT**Message Meaning:** FDS statistics sent**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16



Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32031 - LOG\_ID\_VIEW\_MEM\_LOG\_FAIL

**Message ID:** 32031

**Message Description:** LOG\_ID\_VIEW\_MEM\_LOG\_FAIL

**Message Meaning:** Memory log access failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 32032 - LOG\_ID\_DISK\_DLP\_ARCH\_FULL

**Message ID:** 32032

**Message Description:** LOG\_ID\_DISK\_DLP\_ARCH\_FULL

**Message Meaning:** DLP archive full

**Type:** Event

**Category:** SYSTEM

**Severity:** Emergency

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32033 - LOG\_ID\_DISK\_QUAR\_FULL

**Message ID:** 32033

**Message Description:** LOG\_ID\_DISK\_QUAR\_FULL

**Message Meaning:** Quarantine full

**Type:** Event

**Category:** SYSTEM**Severity:** Emergency

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32034 - LOG\_ID\_DISK\_REPORT\_FULL

**Message ID:** 32034**Message Description:** LOG\_ID\_DISK\_REPORT\_FULL**Message Meaning:** Report full**Type:** Event**Category:** SYSTEM**Severity:** Emergency

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32035 - LOG\_ID\_VDOM\_DISABLED

**Message ID:** 32035

**Message Description:** LOG\_ID\_VDOM\_DISABLED

**Message Meaning:** VDOM disabled

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 32036 - LOG\_ID\_DISK\_IPS\_ARCH\_FULL

**Message ID:** 32036

**Message Description:** LOG\_ID\_DISK\_IPS\_ARCH\_FULL

**Message Meaning:** IPS archive full

**Type:** Event

**Category:** SYSTEM

**Severity:** Emergency

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32037 - LOG\_ID\_DISK\_LOG\_FIRST\_FULL

**Message ID:** 32037

**Message Description:** LOG\_ID\_DISK\_LOG\_FIRST\_FULL

**Message Meaning:** Disk log full over first warning

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32038 - LOG\_ID\_LOG\_ROLL\_FORTICRON

**Message ID:** 32038

**Message Description:** LOG\_ID\_LOG\_ROLL\_FORTICRON

**Message Meaning:** Log rotation requested by FortiCron

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
reason	Reason	string	256
log	Log Name for Log Rotation	string	32

## 32039 - LOG\_ID\_VIEW\_MEM\_LOG\_SUCC

**Message ID:** 32039

**Message Description:** LOG\_ID\_VIEW\_MEM\_LOG\_SUCC

**Message Meaning:** Memory logs viewed successfully

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096
log	Log Name for Log Rotation	string	32

## 32040 - LOG\_ID\_REPORT\_DELETED

**Message ID:** 32040

**Message Description:** LOG\_ID\_REPORT\_DELETED

**Message Meaning:** Report deleted

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 32041 - LOG\_ID\_REPORT\_DELETED\_GUI

**Message ID:** 32041

**Message Description:** LOG\_ID\_REPORT\_DELETED\_GUI

**Message Meaning:** Report deleted from GUI

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32



Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 32042 - LOG\_ID\_MEM\_LOG\_SECOND\_FULL

**Message ID:** 32042

**Message Description:** LOG\_ID\_MEM\_LOG\_SECOND\_FULL

**Message Meaning:** Memory log full over second warning level

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32043 - LOG\_ID\_MEM\_LOG\_FINAL\_FULL

**Message ID:** 32043

**Message Description:** LOG\_ID\_MEM\_LOG\_FINAL\_FULL

**Message Meaning:** Memory log full over final warning level

**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32044 - LOG\_ID\_LOG\_DELETE

**Message ID:** 32044**Message Description:** LOG\_ID\_LOG\_DELETE**Message Meaning:** Log deleted by user**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
log	Log Name for Log Rotation	string	32

## 32045 - LOG\_ID\_MGR\_LIC\_EXPIRE

**Message ID:** 32045

**Message Description:** LOG\_ID\_MGR\_LIC\_EXPIRE

**Message Meaning:** FortiGuard management service license expiring

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32048 - LOG\_ID\_SCHEDULE\_EXPIRE

**Message ID:** 32048

**Message Description:** LOG\_ID\_SCHEDULE\_EXPIRE

**Message Meaning:** One time schedule expiring

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32049 - LOG\_ID\_FC\_EXPIRE

**Message ID:** 32049

**Message Description:** LOG\_ID\_FC\_EXPIRE

**Message Meaning:** FortiCloud license expiring

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32050 - LOG\_ID\_POL\_PKT\_CAPTURE\_FULL

**Message ID:** 32050

**Message Description:** LOG\_ID\_POL\_PKT\_CAPTURE\_FULL

**Message Meaning:** Policy packet capture full

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32051 - LOG\_ID\_LOG\_UPLOAD

**Message ID:** 32051

**Message Description:** LOG\_ID\_LOG\_UPLOAD

**Message Meaning:** Disk logs upload started

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32052 - LOG\_ID\_UPLOAD\_RUN\_SCRIPT

**Message ID:** 32052

**Message Description:** LOG\_ID\_UPLOAD\_RUN\_SCRIPT

**Message Meaning:** Upload and run a script

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 32053 - LOG\_ID\_ADMIN\_MTNER\_LOGIN\_SUCC

**Message ID:** 32053

**Message Description:** LOG\_ID\_ADMIN\_MTNER\_LOGIN\_SUCC

**Message Meaning:** Admin monitor login successful

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
dstip	Destination IP	ip	39
reason	Reason	string	256
sn	Serial Number	string	64
profile	Profile Name	string	64
method	Method	string	64

## 32054 - LOG\_ID\_ADMIN\_MTNER\_LOGOUT

**Message ID:** 32054

**Message Description:** LOG\_ID\_ADMIN\_MTNER\_LOGOUT

**Message Meaning:** Admin monitor logout successful

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11



Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
dstip	Destination IP	ip	39
reason	Reason	string	256
duration	Duration	uint32	10
sn	Serial Number	string	64
method	Method	string	64
state	State	string	64

## 32057 - LOG\_ID\_VIEW\_FAZ\_LOG\_FAIL

**Message ID:** 32057

**Message Description:** LOG\_ID\_VIEW\_FAZ\_LOG\_FAIL

**Message Meaning:** FortiAnalyzer log access failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 32058 - LOG\_ID\_VIEW\_FAZ\_LOG\_SUCC

**Message ID:** 32058

**Message Description:** LOG\_ID\_VIEW\_FAZ\_LOG\_SUCC

**Message Meaning:** FortiAnalyzer logs viewed successfully

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 32095 - LOG\_ID\_GUI\_CHG\_SUB\_MODULE

**Message ID:** 32095

**Message Description:** LOG\_ID\_GUI\_CHG\_SUB\_MODULE

**Message Meaning:** Admin performed an action from GUI

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32096 - LOG\_ID\_GUI\_DOWNLOAD\_LOG

**Message ID:** 32096

**Message Description:** LOG\_ID\_GUI\_DOWNLOAD\_LOG**Message Meaning:** Log file downloaded from GUI**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 32097 - LOG\_ID\_DELETE\_CAPTURE\_PKT

**Message ID:** 32097**Message Description:** LOG\_ID\_DELETE\_CAPTURE\_PKT**Message Meaning:** Policy packet capture file deleted**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32100 - LOG\_ID\_FORTI\_TOKEN\_SYNC

**Message ID:** 32100

**Message Description:** LOG\_ID\_FORTI\_TOKEN\_SYNC

**Message Meaning:** FortiToken synchronized

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 32102 - LOG\_ID\_CHG\_CONFIG

**Message ID:** 32102

**Message Description:** LOG\_ID\_CHG\_CONFIG

**Message Meaning:** Configuration changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
module	Configuration Module Name	string	32
submodule	Sub-module name. For example autoupdate is sub-module in log of "config system autoupdate schedule"	string	32

## 32103 - LOG\_ID\_NEW\_FIRMWARE

**Message ID:** 32103

**Message Description:** LOG\_ID\_NEW\_FIRMWARE

**Message Meaning:** New firmware available on FortiGuard

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32104 - LOG\_ID\_CHG\_CONFIG\_GUI

**Message ID:** 32104

**Message Description:** LOG\_ID\_CHG\_CONFIG\_GUI

**Message Meaning:** Configuration changed via GUI

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096
module	Configuration Module Name	string	32
submodule	Sub-module name. For example autoupdate is sub-module in log of "config system autoupdate schedule"	string	32

## 32105 - LOG\_ID\_NTP\_SVR\_STAUS\_CHG\_REACHABLE

**Message ID:** 32105

**Message Description:** LOG\_ID\_NTP\_SVR\_STAUS\_CHG\_REACHABLE

**Message Meaning:** NTP server status changes to reachable

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10



Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096
field	NTP date-time field	string	32

## 32106 - LOG\_ID\_NTP\_SVR\_STAUS\_CHG\_RESOLVABLE

**Message ID:** 32106

**Message Description:** LOG\_ID\_NTP\_SVR\_STAUS\_CHG\_RESOLVABLE

**Message Meaning:** NTP server status changes to resolvable

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096
field	NTP date-time field	string	32

## 32107 - LOG\_ID\_NTP\_SVR\_STAUS\_CHG\_UNRESOLVABLE

**Message ID:** 32107

**Message Description:** LOG\_ID\_NTP\_SVR\_STAUS\_CHG\_UNRESOLVABLE

**Message Meaning:** NTP server status changes to unresolvable

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
field	NTP date-time field	string	32

## 32108 - LOG\_ID\_NTP\_SVR\_STAUS\_CHG\_UNREACHABLE

**Message ID:** 32108

**Message Description:** LOG\_ID\_NTP\_SVR\_STAUS\_CHG\_UNREACHABLE

**Message Meaning:** NTP server status changes to unreachable

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096
field	NTP date-time field	string	32

## 32109 - LOG\_ID\_UPD\_SIGN\_AV\_DB

**Message ID:** 32109

**Message Description:** LOG\_ID\_UPD\_SIGN\_AV\_DB

**Message Meaning:** Updating virus database

**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32110 - LOG\_ID\_UPD\_SIGN\_IPS\_DB

**Message ID:** 32110**Message Description:** LOG\_ID\_UPD\_SIGN\_IPS\_DB**Message Meaning:** IPS database updated**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32111 - LOG\_ID\_UPD\_SIGN\_AVIPS\_DB

**Message ID:** 32111

**Message Description:** LOG\_ID\_UPD\_SIGN\_AVIPS\_DB

**Message Meaning:** AV, IPS, GeoIP, SRC-VIS, FortiFlow, URL White-list, Certificate databases updated

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

### 32113 - LOG\_ID\_UPD\_SIGN\_SRCVIS\_DB

**Message ID:** 32113

**Message Description:** LOG\_ID\_UPD\_SIGN\_SRCVIS\_DB

**Message Meaning:** SRC-VIS object updated

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32114 - LOG\_ID\_UPD\_SIGN\_GEOIP\_DB

**Message ID:** 32114

**Message Description:** LOG\_ID\_UPD\_SIGN\_GEOIP\_DB

**Message Meaning:** GeoIP object updated

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32116 - LOG\_ID\_UPD\_SIGN\_AVPKG\_FAILURE

**Message ID:** 32116

**Message Description:** LOG\_ID\_UPD\_SIGN\_AVPKG\_FAILURE

**Message Meaning:** AV package update by SCP failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32117 - LOG\_ID\_UPD\_SIGN\_AVPKG\_SUCCESS

**Message ID:** 32117

**Message Description:** LOG\_ID\_UPD\_SIGN\_AVPKG\_SUCCESS

**Message Meaning:** AV package update by SCP successful

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11



Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32118 - LOG\_ID\_UPD\_ADMIN\_AV\_DB

**Message ID:** 32118

**Message Description:** LOG\_ID\_UPD\_ADMIN\_AV\_DB

**Message Meaning:** AV updated by admin

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096

## 32119 - LOG\_ID\_UPD\_SCANUNIT\_AV\_DB

**Message ID:** 32119

**Message Description:** LOG\_ID\_UPD\_SCANUNIT\_AV\_DB

**Message Meaning:** AV database updated by scanunit

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32120 - LOG\_ID\_RPT\_ADD\_DATASET

**Message ID:** 32120

**Message Description:** LOG\_ID\_RPT\_ADD\_DATASET

**Message Meaning:** Report data set added

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096
name	Display Name of the Connection	string	128

## 32122 - LOG\_ID\_RPT\_DEL\_DATASET

**Message ID:** 32122

**Message Description:** LOG\_ID\_RPT\_DEL\_DATASET

**Message Meaning:** Report data set deleted

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096
name	Display Name of the Connection	string	128

## 32125 - LOG\_ID\_RPT\_ADD\_CHART

**Message ID:** 32125

**Message Description:** LOG\_ID\_RPT\_ADD\_CHART

**Message Meaning:** Report chart widget added

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
msg	Log Message	string	4096
name	Display Name of the Connection	string	128

## 32126 - LOG\_ID\_RPT\_DEL\_CHART

**Message ID:** 32126

**Message Description:** LOG\_ID\_RPT\_DEL\_CHART

**Message Meaning:** Report chart widget deleted

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096
name	Display Name of the Connection	string	128

## 32129 - LOG\_ID\_ADD\_GUEST

**Message ID:** 32129

**Message Description:** LOG\_ID\_ADD\_GUEST

**Message Meaning:** Guest user added

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
status	Status	string	23
msg	Log Message	string	4096
name	Display Name of the Connection	string	128

## 32130 - LOG\_ID\_CHG\_USER

**Message ID:** 32130

**Message Description:** LOG\_ID\_CHG\_USER

**Message Meaning:** User changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096
name	Display Name of the Connection	string	128
new_status	New Status	string	512
old_status	Original Status	string	512
passwd	Password	string	20

## 32131 - LOG\_ID\_DEL\_GUEST

**Message ID:** 32131

**Message Description:** LOG\_ID\_DEL\_GUEST

**Message Meaning:** Guest user deleted

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
status	Status	string	23
msg	Log Message	string	4096
name	Display Name of the Connection	string	128

## 32132 - LOG\_ID\_ADD\_USER

**Message ID:** 32132

**Message Description:** LOG\_ID\_ADD\_USER

**Message Meaning:** Local user added

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20



Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
status	Status	string	23
msg	Log Message	string	4096
name	Display Name of the Connection	string	128

## 32138 - LOG\_ID\_REBOOT

**Message ID:** 32138

**Message Description:** LOG\_ID\_REBOOT

**Message Meaning:** Device rebooted

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32139 - LOG\_ID\_WAKE\_ON\_LAN

**Message ID:** 32139

**Message Description:** LOG\_ID\_WAKE\_ON\_LAN

**Message Meaning:** Wake on LAN device

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32140 - LOG\_ID\_TIME\_USER\_SETTING\_CHG

**Message ID:** 32140

**Message Description:** LOG\_ID\_TIME\_USER\_SETTING\_CHG

**Message Meaning:** Global time setting changed by user

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
srcip	Source IP	ip	39
field	NTP date-time field	string	32

## 32141 - LOG\_ID\_TIME\_NTP\_SETTING\_CHG

**Message ID:** 32141

**Message Description:** LOG\_ID\_TIME\_NTP\_SETTING\_CHG

**Message Meaning:** Global time setting changed by NTP

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096
field	NTP date-time field	string	32

## 32142 - LOG\_ID\_BACKUP\_CONF

**Message ID:** 32142

**Message Description:** LOG\_ID\_BACKUP\_CONF

**Message Meaning:** System configuration backed up

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

### 32143 - LOG\_ID\_BACKUP\_CONF\_BY\_SCP

**Message ID:** 32143

**Message Description:** LOG\_ID\_BACKUP\_CONF\_BY\_SCP

**Message Meaning:** System configuration backed up by SCP

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32144 - LOG\_ID\_BACKUP\_CONF\_ERROR

**Message ID:** 32144

**Message Description:** LOG\_ID\_BACKUP\_CONF\_ERROR

**Message Meaning:** System configuration backed up error

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32145 - LOG\_ID\_BACKUP\_CONF\_ALERT

**Message ID:** 32145

**Message Description:** LOG\_ID\_BACKUP\_CONF\_ALERT

**Message Meaning:** System configuration backed up alert

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32146 - LOG\_ID\_TIME\_PTP\_SETTING\_CHG

**Message ID:** 32146

**Message Description:** LOG\_ID\_TIME\_PTP\_SETTING\_CHG

**Message Meaning:** Global time setting changed by PTP

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
field	NTP date-time field	string	32

## 32148 - LOG\_ID\_GET\_CRL

**Message ID:** 32148

**Message Description:** LOG\_ID\_GET\_CRL

**Message Meaning:** CRL update requested

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
crl	Certificate revocation lists	string	4096



## 32149 - LOG\_ID\_COMMAND\_FAIL

**Message ID:** 32149

**Message Description:** LOG\_ID\_COMMAND\_FAIL

**Message Meaning:** Command failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 32151 - LOG\_ID\_ADD\_IP6\_LOCAL\_POL

**Message ID:** 32151

**Message Description:** LOG\_ID\_ADD\_IP6\_LOCAL\_POL

**Message Meaning:** IPv6 firewall local in policy added

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
act	Action	string	16
daddr	Destination address	string	80
dintf	Destination interface	string	36
iptype	IP type	string	16

## 32152 - LOG\_ID\_CHG\_IP6\_LOCAL\_POL

**Message ID:** 32152

**Message Description:** LOG\_ID\_CHG\_IP6\_LOCAL\_POL

**Message Meaning:** IPv6 firewall local in policy setting changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
act	Action	string	16
daddr	Destination address	string	80
dintf	Destination interface	string	36
iptype	IP type	string	16

## 32153 - LOG\_ID\_DEL\_IP6\_LOCAL\_POL

**Message ID:** 32153

**Message Description:** LOG\_ID\_DEL\_IP6\_LOCAL\_POL

**Message Meaning:** IPv6 firewall local in policy deleted

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
act	Action	string	16

Log Field Name	Description	Data Type	Length
daddr	Destination address	string	80
dintf	Destination interface	string	36
iptype	IP type	string	16

## 32155 - LOG\_ID\_ACT\_FTOKEN\_REQ

**Message ID:** 32155

**Message Description:** LOG\_ID\_ACT\_FTOKEN\_REQ

**Message Meaning:** FortiToken activation requested

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
serialno	Serial Number	string	16

## 32156 - LOG\_ID\_ACT\_FTOKEN\_SUCC

**Message ID:** 32156

**Message Description:** LOG\_ID\_ACT\_FTOKEN\_SUCC**Message Meaning:** FortiToken activation successful**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
serialno	Serial Number	string	16

## 32157 - LOG\_ID\_SYNC\_FTOKEN\_SUCC

**Message ID:** 32157**Message Description:** LOG\_ID\_SYNC\_FTOKEN\_SUCC**Message Meaning:** FortiToken re-synchronized**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
serialno	Serial Number	string	16

## 32158 - LOG\_ID\_SYNC\_FTOKEN\_FAIL

**Message ID:** 32158

**Message Description:** LOG\_ID\_SYNC\_FTOKEN\_FAIL

**Message Meaning:** FortiToken re-synchronization failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
serialno	Serial Number	string	16

## 32159 - LOG\_ID\_ACT\_FTOKEN\_FAIL

**Message ID:** 32159

**Message Description:** LOG\_ID\_ACT\_FTOKEN\_FAIL

**Message Meaning:** FortiToken activation failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
serialno	Serial Number	string	16

## 32160 - LOG\_ID\_FTM\_PUSH\_SUCC

**Message ID:** 32160

**Message Description:** LOG\_ID\_FTM\_PUSH\_SUCC

**Message Meaning:** FortiToken mobile push message succeeded

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32161 - LOG\_ID\_FTM\_PUSH\_FAIL

**Message ID:** 32161

**Message Description:** LOG\_ID\_FTM\_PUSH\_FAIL



**Message Meaning:** FortiToken mobile push message failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32168 - LOG\_ID\_REACH\_VDOM\_LIMIT

**Message ID:** 32168

**Message Description:** LOG\_ID\_REACH\_VDOM\_LIMIT

**Message Meaning:** VDOM limit reached

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 32169 - LOG\_ID\_ALARM\_DLP\_DB

**Message ID:** 32169

**Message Description:** LOG\_ID\_ALARM\_DLP\_DB

**Message Meaning:** DLP database space alarm

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 32170 - LOG\_ID\_ALARM\_MSG

**Message ID:** 32170

**Message Description:** LOG\_ID\_ALARM\_MSG

**Message Meaning:** Alarm created

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
alarmid	Alarm ID	uint32	10
groupid	User Group ID	uint32	10

## 32171 - LOG\_ID\_ALARM\_ACK

**Message ID:** 32171

**Message Description:** LOG\_ID\_ALARM\_ACK

**Message Meaning:** Alarm acknowledged

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
alarmid	Alarm ID	uint32	10
acktime	Alarm Acknowledge Time	string	24

## 32172 - LOG\_ID\_ADD\_IP4\_LOCAL\_POL

**Message ID:** 32172

**Message Description:** LOG\_ID\_ADD\_IP4\_LOCAL\_POL

**Message Meaning:** IPv4 firewall local in policy added

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
act	Action	string	16
daddr	Destination address	string	80
dintf	Destination interface	string	36
iptype	IP type	string	16

## 32173 - LOG\_ID\_CHG\_IP4\_LOCAL\_POL

**Message ID:** 32173

**Message Description:** LOG\_ID\_CHG\_IP4\_LOCAL\_POL

**Message Meaning:** IPv4 firewall local in policy's setting changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
act	Action	string	16
daddr	Destination address	string	80
dintf	Destination interface	string	36
iptype	IP type	string	16

## 32174 - LOG\_ID\_DEL\_IP4\_LOCAL\_POL

**Message ID:** 32174

**Message Description:** LOG\_ID\_DEL\_IP4\_LOCAL\_POL

**Message Meaning:** IPv4 firewall local in policy deleted

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
act	Action	string	16
daddr	Destination address	string	80
dintf	Destination interface	string	36
iptype	IP type	string	16

## 32190 - LOG\_ID\_UPT\_INVALID\_IMG

**Message ID:** 32190

**Message Description:** LOG\_ID\_UPT\_INVALID\_IMG

**Message Meaning:** Invalid image loaded

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32191 - LOG\_ID\_UPT\_INVALID\_IMG\_CC

**Message ID:** 32191

**Message Description:** LOG\_ID\_UPT\_INVALID\_IMG\_CC

**Message Meaning:** Image with invalid CC signature loaded

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32192 - LOG\_ID\_UPT\_INVALID\_IMG\_RSA

**Message ID:** 32192

**Message Description:** LOG\_ID\_UPT\_INVALID\_IMG\_RSA

**Message Meaning:** Image with invalid RSA signature loaded

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11



Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32193 - LOG\_ID\_UPT\_IMG\_RSA

**Message ID:** 32193

**Message Description:** LOG\_ID\_UPT\_IMG\_RSA

**Message Meaning:** Image with valid RSA signature loaded

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32194 - LOG\_ID\_UPT\_IMG\_FAIL

**Message ID:** 32194

**Message Description:** LOG\_ID\_UPT\_IMG\_FAIL

**Message Meaning:** System upgrade failed due to file operation failure

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32199 - LOG\_ID\_RESTORE\_IMG\_USB

**Message ID:** 32199

**Message Description:** LOG\_ID\_RESTORE\_IMG\_USB

**Message Meaning:** Image restored from USB

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32200 - LOG\_ID\_SHUTDOWN

**Message ID:** 32200

**Message Description:** LOG\_ID\_SHUTDOWN

**Message Meaning:** Device shutdown

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32201 - LOG\_ID\_LOAD\_IMG\_SUCC

**Message ID:** 32201

**Message Description:** LOG\_ID\_LOAD\_IMG\_SUCC

**Message Meaning:** Image loaded successfully

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32202 - LOG\_ID\_RESTORE\_IMG

**Message ID:** 32202

**Message Description:** LOG\_ID\_RESTORE\_IMG

**Message Meaning:** Image restored

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32203 - LOG\_ID\_RESTORE\_CONF

**Message ID:** 32203

**Message Description:** LOG\_ID\_RESTORE\_CONF

**Message Meaning:** Configuration restored

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32204 - LOG\_ID\_RESTORE\_FGD\_SVR

**Message ID:** 32204

**Message Description:** LOG\_ID\_RESTORE\_FGD\_SVR

**Message Meaning:** FortiGuard service restored

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32205 - LOG\_ID\_RESTORE\_VDOM\_LIC

**Message ID:** 32205

**Message Description:** LOG\_ID\_RESTORE\_VDOM\_LIC

**Message Meaning:** VM license restored

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32206 - LOG\_ID\_RESTORE\_SCRIPT

**Message ID:** 32206

**Message Description:** LOG\_ID\_RESTORE\_SCRIPT

**Message Meaning:** Script restored from management station

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32



Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32207 - LOG\_ID\_RETRIEVE\_CONF\_LIST

**Message ID:** 32207

**Message Description:** LOG\_ID\_RETRIEVE\_CONF\_LIST

**Message Meaning:** Configuration list retrieval failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32208 - LOG\_ID\_IMP\_PKCS12\_CERT

**Message ID:** 32208

**Message Description:** LOG\_ID\_IMP\_PKCS12\_CERT

**Message Meaning:** PKCS12 certificate imported

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32209 - LOG\_ID\_RESTORE\_USR\_DEF\_IPS

**Message ID:** 32209

**Message Description:** LOG\_ID\_RESTORE\_USR\_DEF\_IPS

**Message Meaning:** IPS custom signatures restored

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32210 - LOG\_ID\_BACKUP\_IMG\_SUCC

**Message ID:** 32210

**Message Description:** LOG\_ID\_BACKUP\_IMG\_SUCC

**Message Meaning:** Firmware image backed up successfully

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32211 - LOG\_ID\_UPLOAD\_REVISION

**Message ID:** 32211

**Message Description:** LOG\_ID\_UPLOAD\_REVISION

**Message Meaning:** Revision uploaded to flash disk

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32212 - LOG\_ID\_DEL\_REVISION

**Message ID:** 32212

**Message Description:** LOG\_ID\_DEL\_REVISION

**Message Meaning:** Revision deleted

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32213 - LOG\_ID\_RESTORE\_TEMPLATE

**Message ID:** 32213

**Message Description:** LOG\_ID\_RESTORE\_TEMPLATE

**Message Meaning:** Template restored

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 32214 - LOG\_ID\_RESTORE\_FILE

**Message ID:** 32214

**Message Description:** LOG\_ID\_RESTORE\_FILE

**Message Meaning:** File restore failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 32215 - LOG\_ID\_UPT\_IMG

**Message ID:** 32215

**Message Description:** LOG\_ID\_UPT\_IMG

**Message Meaning:** Image updated

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32217 - LOG\_ID\_UPD\_IPS

**Message ID:** 32217

**Message Description:** LOG\_ID\_UPD\_IPS

**Message Meaning:** IPS package - Admin update successful

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096



## 32218 - LOG\_ID\_UPD\_DLP

**Message ID:** 32218

**Message Description:** LOG\_ID\_UPD\_DLP

**Message Meaning:** DLP fingerprint database update via SCP failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32219 - LOG\_ID\_BACKUP\_OUTPUT

**Message ID:** 32219

**Message Description:** LOG\_ID\_BACKUP\_OUTPUT

**Message Meaning:** Error output backup via SCP successful

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32220 - LOG\_ID\_BACKUP\_COMMAND

**Message ID:** 32220

**Message Description:** LOG\_ID\_BACKUP\_COMMAND

**Message Meaning:** Batch mode command output backup via SCP successful

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32221 - LOG\_ID\_UPD\_VDOM\_LIC

**Message ID:** 32221

**Message Description:** LOG\_ID\_UPD\_VDOM\_LIC

**Message Meaning:** VM license installed via SCP

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32222 - LOG\_ID\_GLB\_SETTING\_CHG

**Message ID:** 32222

**Message Description:** LOG\_ID\_GLB\_SETTING\_CHG

**Message Meaning:** Global setting changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
field	NTP date-time field	string	32
old_value	Original Virtual Domain name	string	128
new_value	New Virtual Domain Name	string	128

## 32223 - LOG\_ID\_BACKUP\_USER\_DEF\_IPS

**Message ID:** 32223

**Message Description:** LOG\_ID\_BACKUP\_USER\_DEF\_IPS

**Message Meaning:** IPS custom signatures backup success

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32224 - LOG\_ID\_BACKUP\_DISK\_LOG

**Message ID:** 32224

**Message Description:** LOG\_ID\_BACKUP\_DISK\_LOG

**Message Meaning:** Disk logs backed up

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
file	Report file full path	string	256
hash	Hash Value of Downloaded File	string	32

## 32225 - LOG\_ID\_DEL\_ALL\_REVISION

**Message ID:** 32225

**Message Description:** LOG\_ID\_DEL\_ALL\_REVISION

**Message Meaning:** Revision database reset due to data corruption

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32226 - LOG\_ID\_LOAD\_IMG\_FAIL

**Message ID:** 32226

**Message Description:** LOG\_ID\_LOAD\_IMG\_FAIL

**Message Meaning:** Image failed to load

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32227 - LOG\_ID\_UPD\_DLP\_FAIL

**Message ID:** 32227

**Message Description:** LOG\_ID\_UPD\_DLP\_FAIL

**Message Meaning:** DLP fingerprint database failed to update by SCP

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096



## 32228 - LOG\_ID\_LOAD\_IMG\_FAIL\_WRONG\_IMG

**Message ID:** 32228

**Message Description:** LOG\_ID\_LOAD\_IMG\_FAIL\_WRONG\_IMG

**Message Meaning:** Firmware image loaded incorrect

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 32229 - LOG\_ID\_LOAD\_IMG\_FAIL\_NO\_RSA

**Message ID:** 32229

**Message Description:** LOG\_ID\_LOAD\_IMG\_FAIL\_NO\_RSA

**Message Meaning:** Firmware image without valid RSA signature loaded

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 32230 - LOG\_ID\_LOAD\_IMG\_FAIL\_INVALID\_RSA

**Message ID:** 32230

**Message Description:** LOG\_ID\_LOAD\_IMG\_FAIL\_INVALID\_RSA

**Message Meaning:** Firmware image with invalid RSA signature loaded

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 32231 - LOG\_ID\_RESTORE\_FGD\_SVR\_FAIL

**Message ID:** 32231

**Message Description:** LOG\_ID\_RESTORE\_FGD\_SVR\_FAIL

**Message Meaning:** FortiGuard service failed to restore

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32232 - LOG\_ID\_RESTORE\_VDOM\_LIC\_FAIL

**Message ID:** 32232

**Message Description:** LOG\_ID\_RESTORE\_VDOM\_LIC\_FAIL

**Message Meaning:** VM license failed to restore

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32233 - LOG\_ID\_BACKUP\_IMG\_FAIL

**Message ID:** 32233

**Message Description:** LOG\_ID\_BACKUP\_IMG\_FAIL

**Message Meaning:** Firmware image backup failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32234 - LOG\_ID\_RESTORE\_IMG\_INVALID\_CC

**Message ID:** 32234

**Message Description:** LOG\_ID\_RESTORE\_IMG\_INVALID\_CC

**Message Meaning:** Image with invalid CC signature restored

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 32235 - LOG\_ID\_RESTORE\_IMG\_FORTIGUARD

**Message ID:** 32235

**Message Description:** LOG\_ID\_RESTORE\_IMG\_FORTIGUARD

**Message Meaning:** Image restored from FortiGuard Management

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
msg	Log Message	string	4096

## 32236 - LOG\_ID\_BACKUP\_MEM\_LOG

**Message ID:** 32236

**Message Description:** LOG\_ID\_BACKUP\_MEM\_LOG

**Message Meaning:** Memory logs backed up

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32237 - LOG\_ID\_BACKUP\_MEM\_LOG\_FAIL

**Message ID:** 32237

**Message Description:** LOG\_ID\_BACKUP\_MEM\_LOG\_FAIL

**Message Meaning:** Memory logs failed to back up

**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32238 - LOG\_ID\_BACKUP\_DISK\_LOG\_FAIL

**Message ID:** 32238**Message Description:** LOG\_ID\_BACKUP\_DISK\_LOG\_FAIL**Message Meaning:** Disk logs failed to back up**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10



Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32239 - LOG\_ID\_BACKUP\_DISK\_LOG\_USB

**Message ID:** 32239

**Message Description:** LOG\_ID\_BACKUP\_DISK\_LOG\_USB

**Message Meaning:** Disk logs backed up to USB

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32240 - LOG\_ID\_SYS\_USB\_MODE

**Message ID:** 32240

**Message Description:** LOG\_ID\_SYS\_USB\_MODE

**Message Meaning:** System operating in USB mode

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32241 - LOG\_ID\_BACKUP\_DISK\_LOG\_USB\_FAIL

**Message ID:** 32241

**Message Description:** LOG\_ID\_BACKUP\_DISK\_LOG\_USB\_FAIL

**Message Meaning:** Disk logs failed to back up to USB

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32242 - LOG\_ID\_UPD\_VDOM\_LIC\_FAIL

**Message ID:** 32242

**Message Description:** LOG\_ID\_UPD\_VDOM\_LIC\_FAIL

**Message Meaning:** VM license failed to install via SCP

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32243 - LOG\_ID\_UPD\_IPS\_SCP

**Message ID:** 32243

**Message Description:** LOG\_ID\_UPD\_IPS\_SCP

**Message Meaning:** IPS package updated via SCP

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32244 - LOG\_ID\_UPD\_IPS\_SCP\_FAIL

**Message ID:** 32244

**Message Description:** LOG\_ID\_UPD\_IPS\_SCP\_FAIL

**Message Meaning:** IPS package failed to update via SCP

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32245 - LOG\_ID\_BACKUP\_USER\_DEF\_IPS\_FAIL

**Message ID:** 32245

**Message Description:** LOG\_ID\_BACKUP\_USER\_DEF\_IPS\_FAIL

**Message Meaning:** IPS custom signatures backup failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32246 - LOG\_ID\_RESTORE\_USR\_DEF\_IPS\_CRITICAL

**Message ID:** 32246

**Message Description:** LOG\_ID\_RESTORE\_USR\_DEF\_IPS\_CRITICAL**Message Meaning:** IPS custom signatures restored critical**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32247 - LOG\_ID\_SSH\_NEGOTIATION\_FAILURE

**Message ID:** 32247**Message Description:** LOG\_ID\_SSH\_NEGOTIATION\_FAILURE**Message Meaning:** SSH protocol cannot be negotiated**Type:** Event**Category:** SYSTEM**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
port	Port Number	uint16	5
addr	IP Address	string	80

## 32252 - LOG\_ID\_FACTORY\_RESET

**Message ID:** 32252

**Message Description:** LOG\_ID\_FACTORY\_RESET

**Message Meaning:** Factory settings reset

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16



Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32253 - LOG\_ID\_FORMAT\_RAID

**Message ID:** 32253

**Message Description:** LOG\_ID\_FORMAT\_RAID

**Message Meaning:** RAID disk formatted

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
msg	Log Message	string	4096

## 32254 - LOG\_ID\_ENABLE\_RAID

**Message ID:** 32254

**Message Description:** LOG\_ID\_ENABLE\_RAID

**Message Meaning:** RAID enabled

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32255 - LOG\_ID\_DISABLE\_RAID

**Message ID:** 32255

**Message Description:** LOG\_ID\_DISABLE\_RAID

**Message Meaning:** RAID disabled

**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32262 - LOG\_ID\_RESTORE\_IMG\_CONFIRM

**Message ID:** 32262**Message Description:** LOG\_ID\_RESTORE\_IMG\_CONFIRM**Message Meaning:** Image restore confirmed by user**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32300 - LOG\_ID\_UPLOAD\_RPT\_IMG

**Message ID:** 32300

**Message Description:** LOG\_ID\_UPLOAD\_RPT\_IMG

**Message Meaning:** Report image file uploaded

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256

## 32301 - LOG\_ID\_ADD\_VDOM

**Message ID:** 32301

**Message Description:** LOG\_ID\_ADD\_VDOM

**Message Meaning:** VDOM added

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32302 - LOG\_ID\_DEL\_VDOM

**Message ID:** 32302

**Message Description:** LOG\_ID\_DEL\_VDOM

**Message Meaning:** VDOM deleted

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32545 - LOG\_ID\_SYS\_RESTART

**Message ID:** 32545

**Message Description:** LOG\_ID\_SYS\_RESTART

**Message Meaning:** Scheduled daily reboot started

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32546 - LOG\_ID\_APPLICATION\_CRASH

**Message ID:** 32546

**Message Description:** LOG\_ID\_APPLICATION\_CRASH

**Message Meaning:** Application crashed

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 32547 - LOG\_ID\_AUTOSCRIPT\_START

**Message ID:** 32547

**Message Description:** LOG\_ID\_AUTOSCRIPT\_START

**Message Meaning:** Autoscrypt start

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5



Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32548 - LOG\_ID\_AUTOSCRIPT\_STOP

**Message ID:** 32548

**Message Description:** LOG\_ID\_AUTOSCRIPT\_STOP

**Message Meaning:** Autoscript stop

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32549 - LOG\_ID\_AUTOSCRIPT\_STOP\_AUTO

**Message ID:** 32549

**Message Description:** LOG\_ID\_AUTOSCRIPT\_STOP\_AUTO

**Message Meaning:** Autoscript stop automatically

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32550 - LOG\_ID\_AUTOSCRIPT\_DELETE\_RSLT

**Message ID:** 32550

**Message Description:** LOG\_ID\_AUTOSCRIPT\_DELETE\_RSLT

**Message Meaning:** Autoscript delete result

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32551 - LOG\_ID\_AUTOSCRIPT\_BACKUP\_RSLT

**Message ID:** 32551

**Message Description:** LOG\_ID\_AUTOSCRIPT\_BACKUP\_RSLT

**Message Meaning:** Autoscript backup result

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32552 - LOG\_ID\_AUTOSCRIPT\_CHECK\_STATUS

**Message ID:** 32552

**Message Description:** LOG\_ID\_AUTOSCRIPT\_CHECK\_STATUS

**Message Meaning:** Autoscript check status

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32553 - LOG\_ID\_AUTOSCRIPT\_STOP\_REACH\_LIMIT

**Message ID:** 32553

**Message Description:** LOG\_ID\_AUTOSCRIPT\_STOP\_REACH\_LIMIT

**Message Meaning:** Autoscript stop due to limit reached

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32561 - LOG\_ID\_ADMIN\_LOGOUT\_DISCONNECT

**Message ID:** 32561

**Message Description:** LOG\_ID\_ADMIN\_LOGOUT\_DISCONNECT

**Message Meaning:** Admin disconnected

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
dstip	Destination IP	ip	39
reason	Reason	string	256
duration	Duration	uint32	10
sn	Serial Number	string	64
method	Method	string	64
state	State	string	64

## 32562 - LOG\_ID\_STORE\_CONF\_FAIL\_SPACE

**Message ID:** 32562

**Message Description:** LOG\_ID\_STORE\_CONF\_FAIL\_SPACE

**Message Meaning:** Store config failed - not enough flash space

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 32564 - LOG\_ID\_RESTORE\_CONF\_FAIL

**Message ID:** 32564

**Message Description:** LOG\_ID\_RESTORE\_CONF\_FAIL

**Message Meaning:** Configuration failed to restore

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32565 - LOG\_ID\_RESTORE\_CONF\_BY\_MGMT

**Message ID:** 32565

**Message Description:** LOG\_ID\_RESTORE\_CONF\_BY\_MGMT

**Message Meaning:** Configuration restored from management station

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096



## 32566 - LOG\_ID\_RESTORE\_CONF\_BY\_SCP

**Message ID:** 32566

**Message Description:** LOG\_ID\_RESTORE\_CONF\_BY\_SCP

**Message Meaning:** Configuration restored by SCP

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32567 - LOG\_ID\_RESTORE\_CONF\_BY\_USB

**Message ID:** 32567

**Message Description:** LOG\_ID\_RESTORE\_CONF\_BY\_USB

**Message Meaning:** Configuration restored by USB

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 32568 - LOG\_ID\_DEL\_REVISION\_DB

**Message ID:** 32568

**Message Description:** LOG\_ID\_DEL\_REVISION\_DB

**Message Meaning:** Revision Database deletion

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 32569 - LOG\_ID\_FSW\_SWITCH\_LOG\_EVENT

**Message ID:** 32569

**Message Description:** LOG\_ID\_FSW\_SWITCH\_LOG\_EVENT

**Message Meaning:** Switch-Controller

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Unknown

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64

Log Field Name	Description	Data Type	Length
msg		string	4096
sn		string	64
name		string	128
cfgtid		uint32	10
cfgpath		string	128
cfgattr		string	4096
cfgobj		string	256

## 32570 - LOG\_ID\_ADMIN\_MTNER\_LOGOUT\_DISCONNECT

**Message ID:** 32570

**Message Description:** LOG\_ID\_ADMIN\_MTNER\_LOGOUT\_DISCONNECT

**Message Meaning:** Admin monitor disconnected

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
dstip	Destination IP	ip	39
reason	Reason	string	256
duration	Duration	uint32	10
sn	Serial Number	string	64
method	Method	string	64
state	State	string	64

## 32601 - LOG\_ID\_FGT\_SWITCH\_LOG\_DISCOVER

**Message ID:** 32601

**Message Description:** LOG\_ID\_FGT\_SWITCH\_LOG\_DISCOVER

**Message Meaning:** Switch-Controller discovered

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256

Log Field Name	Description	Data Type	Length
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32602 - LOG\_ID\_FGT\_SWITCH\_LOG\_AUTH

**Message ID:** 32602

**Message Description:** LOG\_ID\_FGT\_SWITCH\_LOG\_AUTH

**Message Meaning:** Switch-Controller authorized

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32603 - LOG\_ID\_FGT\_SWITCH\_LOG\_DEAUTH

**Message ID:** 32603

**Message Description:** LOG\_ID\_FGT\_SWITCH\_LOG\_DEAUTH

**Message Meaning:** Switch-Controller deauthorized

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32604 - LOG\_ID\_FGT\_SWITCH\_LOG\_DELETE

**Message ID:** 32604

**Message Description:** LOG\_ID\_FGT\_SWITCH\_LOG\_DELETE

**Message Meaning:** Switch-Controller deleted

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32605 - LOG\_ID\_FGT\_SWITCH\_LOG\_TUNNEL\_UP

**Message ID:** 32605

**Message Description:** LOG\_ID\_FGT\_SWITCH\_LOG\_TUNNEL\_UP

**Message Meaning:** Switch-Controller Tunnel Up

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20



Log Field Name	Description	Data Type	Length
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32606 - LOG\_ID\_FGT\_SWITCH\_LOG\_TUNNEL\_DOWN

**Message ID:** 32606

**Message Description:** LOG\_ID\_FGT\_SWITCH\_LOG\_TUNNEL\_DOWN

**Message Meaning:** Switch-Controller Tunnel Down

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5

Log Field Name	Description	Data Type	Length
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32607 - LOG\_ID\_FGT\_SWITCH\_PUSH\_IMAGE

**Message ID:** 32607

**Message Description:** LOG\_ID\_FGT\_SWITCH\_PUSH\_IMAGE

**Message Meaning:** Image push to FortiSwitch

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32608 - LOG\_ID\_FGT\_SWITCH\_STAGE\_IMAGE

**Message ID:** 32608

**Message Description:** LOG\_ID\_FGT\_SWITCH\_STAGE\_IMAGE

**Message Meaning:** Image stage to FortiSwitch

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32609 - LOG\_ID\_FGT\_SWITCH\_DISABLE\_DISCOVERY

**Message ID:** 32609

**Message Description:** LOG\_ID\_FGT\_SWITCH\_DISABLE\_DISCOVERY

**Message Meaning:** Disable FortiSwitch Discovery

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096

## 32610 - LOG\_ID\_FGT\_SWITCH\_LOG\_WARNING

**Message ID:** 32610

**Message Description:** LOG\_ID\_FGT\_SWITCH\_LOG\_WARNING

**Message Meaning:** Switch-Controller warning

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16

Log Field Name	Description	Data Type	Length
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096

## 32611 - LOG\_ID\_FGT\_SWITCH\_EXPORT\_POOL

**Message ID:** 32611

**Message Description:** LOG\_ID\_FGT\_SWITCH\_EXPORT\_POOL

**Message Meaning:** Export port to pool

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096

Log Field Name	Description	Data Type	Length
sn		string	64
name		string	128

## 32612 - LOG\_ID\_FGT\_SWITCH\_EXPORT\_VDOM

**Message ID:** 32612

**Message Description:** LOG\_ID\_FGT\_SWITCH\_EXPORT\_VDOM

**Message Meaning:** Export port to vdom

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32613 - LOG\_ID\_FGT\_SWITCH\_REQUEST\_PORT

**Message ID:** 32613

**Message Description:** LOG\_ID\_FGT\_SWITCH\_REQUEST\_PORT

**Message Meaning:** Request port from pool

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096

## 32614 - LOG\_ID\_FGT\_SWITCH\_RETURN\_PORT

**Message ID:** 32614

**Message Description:** LOG\_ID\_FGT\_SWITCH\_RETURN\_PORT

**Message Meaning:** Return port to pool

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10

Log Field Name	Description	Data Type	Length
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096

## 32615 - LOG\_ID\_FGT\_SWITCH\_MAC\_ADD

**Message ID:** 32615

**Message Description:** LOG\_ID\_FGT\_SWITCH\_MAC\_ADD

**Message Meaning:** FortiSwitch MAC add

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5



Log Field Name	Description	Data Type	Length
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32616 - LOG\_ID\_FGT\_SWITCH\_MAC\_DEL

**Message ID:** 32616

**Message Description:** LOG\_ID\_FGT\_SWITCH\_MAC\_DEL

**Message Meaning:** FortiSwitch MAC delete

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32617 - LOG\_ID\_FGT\_SWITCH\_MAC\_MOVE

**Message ID:** 32617

**Message Description:** LOG\_ID\_FGT\_SWITCH\_MAC\_MOVE

**Message Meaning:** FortiSwitch MAC move

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128

## 32693 - LOG\_ID\_FGT\_SWITCH\_GROUP\_SWC

**Message ID:** 32693

**Message Description:** LOG\_ID\_FGT\_SWITCH\_GROUP\_SWC

**Message Meaning:** FortiSwitch switch controller

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128
cfgtid		uint32	10
cfgpath		string	128
cfgattr		string	4096
cfgobj		string	256

## 32694 - LOG\_ID\_FGT\_SWITCH\_GROUP\_POE

**Message ID:** 32694

**Message Description:** LOG\_ID\_FGT\_SWITCH\_GROUP\_POE

**Message Meaning:** FortiSwitch PoE

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date		string	10

Log Field Name	Description	Data Type	Length
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128
cfgtid		uint32	10
cfgpath		string	128
cfgattr		string	4096
cfgobj		string	256

## 32695 - LOG\_ID\_FGT\_SWITCH\_GROUP\_LINK

**Message ID:** 32695

**Message Description:** LOG\_ID\_FGT\_SWITCH\_GROUP\_LINK

**Message Meaning:** FortiSwitch link

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8

Log Field Name	Description	Data Type	Length
logid		string	10
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128
cfgtid		uint32	10
cfgpath		string	128
cfgattr		string	4096
cfgobj		string	256

## 32696 - LOG\_ID\_FGT\_SWITCH\_GROUP\_STP

**Message ID:** 32696

**Message Description:** LOG\_ID\_FGT\_SWITCH\_GROUP\_STP

**Message Meaning:** FortiSwitch spanning Tree

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10

Log Field Name	Description	Data Type	Length
type		string	16
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128
cfgtid		uint32	10
cfgpath		string	128
cfgattr		string	4096
cfgobj		string	256

## 32697 - LOG\_ID\_FGT\_SWITCH\_GROUP\_SWITCH

**Message ID:** 32697

**Message Description:** LOG\_ID\_FGT\_SWITCH\_GROUP\_SWITCH

**Message Meaning:** FortiSwitch switch

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16

Log Field Name	Description	Data Type	Length
subtype		string	20
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128
cftid		uint32	10
cfgpath		string	128
cfgattr		string	4096
cfgobj		string	256

## 32698 - LOG\_ID\_FGT\_SWITCH\_GROUP\_ROUTER

**Message ID:** 32698

**Message Description:** LOG\_ID\_FGT\_SWITCH\_GROUP\_ROUTER

**Message Meaning:** FortiSwitch router

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20

Log Field Name	Description	Data Type	Length
level		string	11
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128
cfgtid		uint32	10
cfgpath		string	128
cfgattr		string	4096
cfgobj		string	256

## 32699 - LOG\_ID\_FGT\_SWITCH\_GROUP\_SYSTEM

**Message ID:** 32699

**Message Description:** LOG\_ID\_FGT\_SWITCH\_GROUP\_SYSTEM

**Message Meaning:** FortiSwitch system

**Type:** Event

**Category:** SWITCH-CONTROLLER

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date		string	10
time		string	8
logid		string	10
type		string	16
subtype		string	20
level		string	11



Log Field Name	Description	Data Type	Length
devid		string	16
vd		string	32
eventtime		uint64	20
tz		string	5
logdesc		string	4096
user		string	256
ui		string	64
msg		string	4096
sn		string	64
name		string	128
cfgtid		uint32	10
cfgpath		string	128
cfgattr		string	4096
cfgobj		string	256

## 32700 - LOG\_ID\_DPDK\_EARLY\_INIT\_FAIL

**Message ID:** 32700

**Message Description:** LOG\_ID\_DPDK\_EARLY\_INIT\_FAIL

**Message Meaning:** DPDK early initialization failed.

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 34415 - LOG\_ID\_NP6\_IPSEC\_ENGINE\_BUSY

**Message ID:** 34415

**Message Description:** LOG\_ID\_NP6\_IPSEC\_ENGINE\_BUSY

**Message Meaning:** NP6 IPsec engine is busy

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 34416 - LOG\_ID\_NP6\_IPSEC\_ENGINE\_POSSIBLY\_LOCKUP

**Message ID:** 34416

**Message Description:** LOG\_ID\_NP6\_IPSEC\_ENGINE\_POSSIBLY\_LOCKUP

**Message Meaning:** NP6 IPsec engine is possibly locked up

**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 34417 - LOG\_ID\_NP6\_IPSEC\_ENGINE\_LOCKUP

**Message ID:** 34417**Message Description:** LOG\_ID\_NP6\_IPSEC\_ENGINE\_LOCKUP**Message Meaning:** NP6 IPsec engine is locked up**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 34418 - LOG\_ID\_NP6\_HPE\_PACKET\_DROP

**Message ID:** 34418

**Message Description:** LOG\_ID\_NP6\_HPE\_PACKET\_DROP

**Message Meaning:** NPU HPE is dropping packets

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 34419 - LOG\_ID\_NP6\_HPE\_PACKET\_FLOOD

**Message ID:** 34419

**Message Description:** LOG\_ID\_NP6\_HPE\_PACKET\_FLOOD

**Message Meaning:** NP6 HPE under a packets flood

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 34428 - LOG\_ID\_NP7\_HPE\_PACKET\_DROP

**Message ID:** 34428

**Message Description:** LOG\_ID\_NP7\_HPE\_PACKET\_DROP

**Message Meaning:** NPU HPE is dropping packets

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 34430 - LOG\_ID\_NP7\_HPE\_PACKET\_FLOOD

**Message ID:** 34430

**Message Description:** LOG\_ID\_NP7\_HPE\_PACKET\_FLOOD

**Message Meaning:** NPU HPE under packet flood

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 35001 - LOG\_ID\_HA\_SYNC\_VIRDB

**Message ID:** 35001

**Message Description:** LOG\_ID\_HA\_SYNC\_VIRDB**Message Meaning:** HA secondary synchronized Virus database**Type:** Event**Category:** HA**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 35002 - LOG\_ID\_HA\_SYNC\_ETDB

**Message ID:** 35002**Message Description:** LOG\_ID\_HA\_SYNC\_ETDB**Message Meaning:** HA secondary synchronized Extended database**Type:** Event**Category:** HA**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

### 35003 - LOG\_ID\_HA\_SYNC\_EXDB

**Message ID:** 35003

**Message Description:** LOG\_ID\_HA\_SYNC\_EXDB

**Message Meaning:** HA secondary synchronized Extreme database

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096



## 35004 - LOG\_ID\_HA\_SYNC\_FLDB

**Message ID:** 35004

**Message Description:** LOG\_ID\_HA\_SYNC\_FLDB

**Message Meaning:** HA secondary synchronized FLDB

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 35005 - LOG\_ID\_HA\_SYNC\_IPS

**Message ID:** 35005

**Message Description:** LOG\_ID\_HA\_SYNC\_IPS

**Message Meaning:** HA secondary synchronized IDS package

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

### 35007 - LOG\_ID\_HA\_SYNC\_AV

**Message ID:** 35007

**Message Description:** LOG\_ID\_HA\_SYNC\_AV

**Message Meaning:** HA secondary synchronized AntiVirus package

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 35009 - LOG\_ID\_HA\_SYNC\_CID

**Message ID:** 35009

**Message Description:** LOG\_ID\_HA\_SYNC\_CID

**Message Meaning:** HA secondary synchronized CID package

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 35011 - LOG\_ID\_HA\_SYNC\_FAIL

**Message ID:** 35011

**Message Description:** LOG\_ID\_HA\_SYNC\_FAIL

**Message Meaning:** HA secondary synchronization failed

**Type:** Event

**Category:** HA

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 35012 - LOG\_ID\_CONF\_SYNC\_FAIL

**Message ID:** 35012

**Message Description:** LOG\_ID\_CONF\_SYNC\_FAIL

**Message Meaning:** Secondary sync failed

**Type:** Event

**Category:** HA

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 35013 - LOG\_ID\_HA\_FAILOVER\_FAIL

**Message ID:** 35013

**Message Description:** LOG\_ID\_HA\_FAILOVER\_FAIL

**Message Meaning:** HA failover failed

**Type:** Event

**Category:** HA

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 35014 - LOG\_ID\_HA\_RESET\_UPTIME

**Message ID:** 35014

**Message Description:** LOG\_ID\_HA\_RESET\_UPTIME

**Message Meaning:** HA reset uptime

**Type:** Event

**Category:** HA

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64

## 35015 - LOG\_ID\_HA\_CLEAR\_HISTORY

**Message ID:** 35015

**Message Description:** LOG\_ID\_HA\_CLEAR\_HISTORY

**Message Meaning:** HA clear history

**Type:** Event

**Category:** HA

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64

## 35016 - LOG\_ID\_HA\_FAILOVER\_SUCCESS

**Message ID:** 35016

**Message Description:** LOG\_ID\_HA\_FAILOVER\_SUCCESS

**Message Meaning:** HA failover success

**Type:** Event

**Category:** HA

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 36881 - LOG\_ID\_EVENT\_SYSTEM\_CFG\_REVERT

**Message ID:** 36881

**Message Description:** LOG\_ID\_EVENT\_SYSTEM\_CFG\_REVERT

**Message Meaning:** Configuration reverted due to timeout

**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 36882 - LOG\_ID\_EVENT\_SYSTEM\_CFG\_MANUALLY\_SAVED

**Message ID:** 36882**Message Description:** LOG\_ID\_EVENT\_SYSTEM\_CFG\_MANUALLY\_SAVED**Message Meaning:** Configuration manually saved**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11



Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
msg	Log Message	string	4096

## 37120 - MESGID\_NEG\_GENERIC\_P1\_NOTIF

**Message ID:** 37120

**Message Description:** MESGID\_NEG\_GENERIC\_P1\_NOTIF

**Message Meaning:** Negotiate IPsec phase 1

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23
result	IPsec VPN negotiation result	string	31
peer_notif	IPsec VPN Peer Notification	string	25

## 37121 - MESGID\_NEG\_GENERIC\_P1\_ERROR

**Message ID:** 37121

**Message Description:** MESGID\_NEG\_GENERIC\_P1\_ERROR

**Message Meaning:** Negotiate IPsec phase 1

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23
result	IPsec VPN negotiation result	string	31
peer_notif	IPsec VPN Peer Notification	string	25

## 37122 - MESGID\_NEG\_GENERIC\_P2\_NOTIF

**Message ID:** 37122

**Message Description:** MESGID\_NEG\_GENERIC\_P2\_NOTIF

**Message Meaning:** Negotiate IPsec phase 2

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23
role	IPsec peer role, initiator or responder	string	9
esptransform	IPsec Phase2 ESP encryption method	string	21
espauth	IPsec Phase2 ESP message authentication code	string	17

## 37123 - MESGID\_NEG\_GENERIC\_P2\_ERROR

**Message ID:** 37123

**Message Description:** MESGID\_NEG\_GENERIC\_P2\_ERROR

**Message Meaning:** Negotiate IPsec phase 2

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256

Log Field Name	Description	Data Type	Length
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23
role	IPsec peer role, initiator or responder	string	9
esptransform	IPsec Phase2 ESP encryption method	string	21
espauth	IPsec Phase2 ESP message authentication code	string	17

## 37124 - MESGID\_NEG\_I\_P1\_ERROR

**Message ID:** 37124

**Message Description:** MESGID\_NEG\_I\_P1\_ERROR

**Message Meaning:** IPsec phase 1 error

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23
peer_notif	IPsec VPN Peer Notification	string	25
reason	Reason	string	256

## 37125 - MESGID\_NEG\_I\_P2\_ERROR

**Message ID:** 37125

**Message Description:** MESGID\_NEG\_I\_P2\_ERROR

**Message Meaning:** IPsec phase 2 error

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23
reason	Reason	string	256

## 37126 - MESGID\_NEG\_NO\_STATE\_ERROR

**Message ID:** 37126

**Message Description:** MESGID\_NEG\_NO\_STATE\_ERROR

**Message Meaning:** IPsec no state error

**Type:** Event

**Category:** VPN

**Severity:** Error



Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23
reason	Reason	string	256

## 37127 - MESGID\_NEG\_PROGRESS\_P1\_NOTIF

**Message ID:** 37127

**Message Description:** MESGID\_NEG\_PROGRESS\_P1\_NOTIF**Message Meaning:** Progress IPsec phase 1**Type:** Event**Category:** VPN**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128

Log Field Name	Description	Data Type	Length
status	Status	string	23
result	IPsec VPN negotiation result	string	31
role	IPsec peer role, initiator or responder	string	9
init		string	6
mode	IPsec VPN ID protection mode	string	12
dir	Direction	string	8
stage		uint8	3
exch	Type of IKE messages exchanged	string	14
version	Version	string	64

## 37128 - MESGID\_NEG\_PROGRESS\_P1\_ERROR

**Message ID:** 37128

**Message Description:** MESGID\_NEG\_PROGRESS\_P1\_ERROR

**Message Meaning:** Progress IPsec phase 1

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23
result	IPsec VPN negotiation result	string	31
role	IPsec peer role, initiator or responder	string	9
init		string	6
mode	IPsec VPN ID protection mode	string	12
dir	Direction	string	8
stage		uint8	3
exch	Type of IKE messages exchanged	string	14
version	Version	string	64

## 37129 - MESGID\_NEG\_PROGRESS\_P2\_NOTIF

**Message ID:** 37129

**Message Description:** MESGID\_NEG\_PROGRESS\_P2\_NOTIF

**Message Meaning:** Progress IPsec phase 2

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23
result	IPsec VPN negotiation result	string	31
role	IPsec peer role, initiator or responder	string	9
init		string	6

Log Field Name	Description	Data Type	Length
mode	IPsec VPN ID protection mode	string	12
dir	Direction	string	8
stage		uint8	3
exch	Type of IKE messages exchanged	string	14
version	Version	string	64

## 37130 - MESGID\_NEG\_PROGRESS\_P2\_ERROR

**Message ID:** 37130

**Message Description:** MESGID\_NEG\_PROGRESS\_P2\_ERROR

**Message Meaning:** Progress IPsec phase 2

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23
result	IPsec VPN negotiation result	string	31
role	IPsec peer role, initiator or responder	string	9
init		string	6
mode	IPsec VPN ID protection mode	string	12
dir	Direction	string	8
stage		uint8	3
exch	Type of IKE messages exchanged	string	14
version	Version	string	64

## 37131 - MESGID\_ESP\_ERROR

**Message ID:** 37131

**Message Description:** MESGID\_ESP\_ERROR

**Message Meaning:** IPsec ESP

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23
error_num	Error Number	string	53
spi	Security Parameter Index	string	16
seq	Sequence	string	512

## 37132 - MESGID\_ESP\_CRITICAL

**Message ID:** 37132



**Message Description:** MESGID\_ESP\_CRITICAL**Message Meaning:** IPsec ESP**Type:** Event**Category:** VPN**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128

Log Field Name	Description	Data Type	Length
status	Status	string	23
error_num	Error Number	string	53
spi	Security Parameter Index	string	16
seq	Sequence	string	512

## 37133 - MESGID\_INSTALL\_SA

**Message ID:** 37133

**Message Description:** MESGID\_INSTALL\_SA

**Message Meaning:** IPsec SA installed

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39

Log Field Name	Description	Data Type	Length
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
role	IPsec peer role, initiator or responder	string	9
in_spi	SPI for incoming traffic	string	16
out_spi	Out SPI	string	16

## 37134 - MESGID\_DELETE\_P1\_SA

**Message ID:** 37134

**Message Description:** MESGID\_DELETE\_P1\_SA

**Message Meaning:** IPsec phase 1 SA deleted

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128

## 37135 - MESGID\_DELETE\_P2\_SA

**Message ID:** 37135

**Message Description:** MESGID\_DELETE\_P2\_SA

**Message Meaning:** IPsec phase 2 SA deleted

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
in_spi	SPI for incoming traffic	string	16
out_spi	Out SPI	string	16

## 37136 - MESGID\_DPD\_FAILURE

**Message ID:** 37136

**Message Description:** MESGID\_DPD\_FAILURE

**Message Meaning:** IPsec DPD failed

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23

## 37137 - MESGID\_CONN\_FAILURE

**Message ID:** 37137

**Message Description:** MESGID\_CONN\_FAILURE

**Message Meaning:** IPsec connection failed**Type:** Event**Category:** VPN**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
status	Status	string	23

## 37138 - MESGID\_CONN\_UPDOWN

**Message ID:** 37138

**Message Description:** MESGID\_CONN\_UPDOWN

**Message Meaning:** IPsec connection status changed

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
tunnelip	IPsec VPN tunnel IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32



Log Field Name	Description	Data Type	Length
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
duration	Duration	uint32	10
sentbyte	Bytes Sent	uint64	20
rcvdbyte	Received Bytes	uint64	20
nextstat	Time interval in seconds for the next statistics	uint32	10

## 37139 - MESGID\_P2\_UPDOWN

**Message ID:** 37139

**Message Description:** MESGID\_P2\_UPDOWN

**Message Meaning:** IPsec phase 2 status changed

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
phase2_name	Phase 2 Name	string	128

## 37141 - MESGID\_CONN\_STATS

**Message ID:** 37141

**Message Description:** MESGID\_CONN\_STATS

**Message Meaning:** IPsec tunnel statistics

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
tunnelip	IPsec VPN tunnel IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
locip	IPsec VPN local gateway IP address	ip	39
remport	Remote Port	uint16	5
locport	Local Port	uint16	5
outintf	IPsec VPN binding interface	string	32
cookies	Cookie	string	64
useralt		string	256
xauthuser	IPsec VPN Xauth user name	string	256
xauthgroup	IPsec VPN Xauth user group name	string	128
assignip	IPsec VPN tunnel assigned IP address	ip	39
vpntunnel	IPsec VPN Tunnel Name	string	128
duration	Duration	uint32	10
sentbyte	Bytes Sent	uint64	20
rcvdbyte	Received Bytes	uint64	20
nextstat	Time interval in seconds for the next statistics	uint32	10

## 37889 - MESGID\_VC\_DELETE

**Message ID:** 37889

**Message Description:** MESGID\_VC\_DELETE**Message Meaning:** Virtual cluster deleted**Type:** Event**Category:** HA**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
vcluster	Virtual cluster	uint32	10

## 37890 - MESGID\_VC\_MOVE\_VDOM

**Message ID:** 37890**Message Description:** MESGID\_VC\_MOVE\_VDOM**Message Meaning:** Virtual cluster VDOM moved**Type:** Event**Category:** HA**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
from_vcluster	Source virtual cluster number	uint32	10
to_vcluster	Destination virtual cluster number	uint32	10
vdname	Virtual Domain Name	string	32

## 37891 - MESGID\_VC\_ADD\_VDOM

**Message ID:** 37891

**Message Description:** MESGID\_VC\_ADD\_VDOM

**Message Meaning:** Virtual cluster VDOM added

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
to_vcluster	Destination virtual cluster number	uint32	10
vdname	Virtual Domain Name	string	32

## 37892 - MESGID\_VC\_MOVE\_MEMB\_STATE

**Message ID:** 37892

**Message Description:** MESGID\_VC\_MOVE\_MEMB\_STATE

**Message Meaning:** Virtual cluster member state moved

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
vcluster_member	Virtual cluster member	uint32	10
vcluster_state	Virtual cluster member state	string	7

## 37893 - MESGID\_VC\_DETECT\_MEMB\_DEAD

**Message ID:** 37893

**Message Description:** MESGID\_VC\_DETECT\_MEMB\_DEAD

**Message Meaning:** Virtual cluster member dead

**Type:** Event

**Category:** HA

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
vcluster	Virtual cluster	uint32	10
ha_group	HA Group Number - can be 0 - 255	uint8	3
sn	Serial Number	string	64

## 37894 - MESGID\_VC\_DETECT\_MEMB\_JOIN

**Message ID:** 37894

**Message Description:** MESGID\_VC\_DETECT\_MEMB\_JOIN

**Message Meaning:** Virtual cluster member joined

**Type:** Event

**Category:** HA

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
vcluster	Virtual cluster	uint32	10
ha_group	HA Group Number - can be 0 - 255	uint8	3
sn	Serial Number	string	64

## 37895 - MESGID\_VC\_ADD\_HADEV

**Message ID:** 37895

**Message Description:** MESGID\_VC\_ADD\_HADEV

**Message Meaning:** Virtual cluster added HA device interface

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32



Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
vcluster	Virtual cluster	uint32	10
devintfname	HA device interface name	string	32

## 37896 - MESGID\_VC\_DEL\_HADEV

**Message ID:** 37896

**Message Description:** MESGID\_VC\_DEL\_HADEV

**Message Meaning:** Virtual cluster deleted HA device interface

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
vcluster	Virtual cluster	uint32	10
devintfname	HA device interface name	string	32

## 37897 - MESGID\_HADEV\_READY

**Message ID:** 37897

**Message Description:** MESGID\_HADEV\_READY

**Message Meaning:** HA device interface ready

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9

## 37898 - MESGID\_HADEV\_FAIL

**Message ID:** 37898

**Message Description:** MESGID\_HADEV\_FAIL

**Message Meaning:** HA device interface failed

**Type:** Event

**Category:** HA

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9

## 37899 - MESGID\_HADEV\_PEERINFO

**Message ID:** 37899

**Message Description:** MESGID\_HADEV\_PEERINFO

**Message Meaning:** HA device interface peer information

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9

## 37900 - MESGID\_HBDEV\_DELETE

**Message ID:** 37900

**Message Description:** MESGID\_HBDEV\_DELETE

**Message Meaning:** Heartbeat device interface deleted

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
devintfname	HA device interface name	string	32

## 37901 - MESGID\_HBDEV\_DOWN

**Message ID:** 37901

**Message Description:** MESGID\_HBDEV\_DOWN

**Message Meaning:** Heartbeat device interface down

**Type:** Event

**Category:** HA

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9

## 37902 - MESGID\_HBDEV\_UP

**Message ID:** 37902

**Message Description:** MESGID\_HBDEV\_UP

**Message Meaning:** Heartbeat device interface up

**Type:** Event

**Category:** HA

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9

## 37903 - MESGID\_SYNC\_STATUS

**Message ID:** 37903

**Message Description:** MESGID\_SYNC\_STATUS

**Message Meaning:** Synchronization status with primary

**Type:** Event

**Category:** HA

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sync_type	The sync type with the primary	string	14
sync_status	The sync status with the primary	string	11

## 37904 - MESGID\_HA\_ACTIVITY

**Message ID:** 37904

**Message Description:** MESGID\_HA\_ACTIVITY

**Message Meaning:** Device set as HA primary

**Type:** Event

**Category:** HA

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
activity	HA activity message	string	128
ip		ip	39
ha-prio	HA Priority	uint8	3

## 37907 - MESGID\_VLAN\_HB\_UP

**Message ID:** 37907

**Message Description:** MESGID\_VLAN\_HB\_UP

**Message Meaning:** VLAN heartbeat started

**Type:** Event

**Category:** HA

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 37908 - MESGID\_VLAN\_HB\_DOWN

**Message ID:** 37908

**Message Description:** MESGID\_VLAN\_HB\_DOWN

**Message Meaning:** VLAN heartbeat lost

**Type:** Event

**Category:** HA

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8



Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

### 37909 - MESGID\_VLAN\_HB\_DOWN\_SUM

**Message ID:** 37909

**Message Description:** MESGID\_VLAN\_HB\_DOWN\_SUM

**Message Meaning:** VLAN heartbeat lost summary

**Type:** Event

**Category:** HA

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 37910 - MESGID\_HB\_PACKET\_LOST

**Message ID:** 37910

**Message Description:** MESGID\_HB\_PACKET\_LOST

**Message Meaning:** Heartbeat packet lost

**Type:** Event

**Category:** HA

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
devintfname	HA device interface name	string	32
ha_role	The HA role in the cluster	string	9

## 37911 - MESGID\_FGSP\_MEMBER\_JOIN

**Message ID:** 37911

**Message Description:** MESGID\_FGSP\_MEMBER\_JOIN

**Message Meaning:** FGSP member joined

**Type:** Event

**Category:** HA

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 37912 - MESGID\_FGSP\_MEMBER\_LEAVE

**Message ID:** 37912

**Message Description:** MESGID\_FGSP\_MEMBER\_LEAVE

**Message Meaning:** FGSP member left

**Type:** Event

**Category:** HA

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 38010 - LOG\_ID\_FIPS\_ENCRY\_FAIL

**Message ID:** 38010

**Message Description:** LOG\_ID\_FIPS\_ENCRY\_FAIL

**Message Meaning:** FIPS CC encryption failed

**Type:** Event

**Category:** USER

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 38011 - LOG\_ID\_FIPS\_DECRY\_FAIL

**Message ID:** 38011

**Message Description:** LOG\_ID\_FIPS\_DECRY\_FAIL**Message Meaning:** FIPS CC decryption failed**Type:** Event**Category:** USER**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
ui	User Interface	string	64

## 38012 - LOG\_ID\_ENTROPY\_TOKEN

**Message ID:** 38012**Message Description:** LOG\_ID\_ENTROPY\_TOKEN**Message Meaning:** Seeding from entropy source**Type:** Event**Category:** USER**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 38031 - LOG\_ID\_FSSO\_LOGON

**Message ID:** 38031

**Message Description:** LOG\_ID\_FSSO\_LOGON

**Message Meaning:** FSSO logon successful

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
server	AD server FQDN or IP	string	64
reason	Reason	string	256

## 38032 - LOG\_ID\_FSSO\_LOGOFF

**Message ID:** 38032

**Message Description:** LOG\_ID\_FSSO\_LOGOFF

**Message Meaning:** FSSO logout successful

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
server	AD server FQDN or IP	string	64
reason	Reason	string	256

### 38033 - LOG\_ID\_FSSO\_SVR\_STATUS

**Message ID:** 38033

**Message Description:** LOG\_ID\_FSSO\_SVR\_STATUS

**Message Meaning:** FSSO Active Directory server authentication status

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65



Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
server	AD server FQDN or IP	string	64

## 38403 - LOGID\_EVENT\_NOTIF\_INSUFFICIENT\_RESOURCE

**Message ID:** 38403

**Message Description:** LOGID\_EVENT\_NOTIF\_INSUFFICIENT\_RESOURCE

**Message Meaning:** Insufficient system resource notification

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 38404 - LOGID\_EVENT\_NOTIF\_HOSTNAME\_ERROR

**Message ID:** 38404

**Message Description:** LOGID\_EVENT\_NOTIF\_HOSTNAME\_ERROR

**Message Meaning:** FortiGuard hostname unresolvable

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
hostname	Hostname	string	128

## 38405 - LOGID\_NOTIF\_CODE\_SENDTO\_SMS\_PHONE

**Message ID:** 38405

**Message Description:** LOGID\_NOTIF\_CODE\_SENDTO\_SMS\_PHONE

**Message Meaning:** Guest user account login information sent to phone

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 38406 - LOGID\_NOTIF\_CODE\_SENDTO\_SMS\_TO

**Message ID:** 38406

**Message Description:** LOGID\_NOTIF\_CODE\_SENDTO\_SMS\_TO

**Message Meaning:** Guest user account login information sent as SMS

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 38407 - LOGID\_NOTIF\_CODE\_SENDTO\_EMAIL

**Message ID:** 38407

**Message Description:** LOGID\_NOTIF\_CODE\_SENDTO\_EMAIL

**Message Meaning:** Guest user account login information sent to email

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 38408 - LOGID\_EVENT\_OFTP\_SSL\_CONNECTED

**Message ID:** 38408

**Message Description:** LOGID\_EVENT\_OFTP\_SSL\_CONNECTED

**Message Meaning:** SSL connection established

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5

## 38409 - LOGID\_EVENT\_OFTP\_SSL\_DISCONNECTED

**Message ID:** 38409

**Message Description:** LOGID\_EVENT\_OFTP\_SSL\_DISCONNECTED

**Message Meaning:** SSL connection closed

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5

## 38410 - LOGID\_EVENT\_OFTP\_SSL\_FAILED

**Message ID:** 38410

**Message Description:** LOGID\_EVENT\_OFTP\_SSL\_FAILED

**Message Meaning:** SSL connection failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
reason	Reason	string	256

## 38411 - LOGID\_EVENT\_TWO\_F\_AUTH\_CODE\_SENDTO

**Message ID:** 38411

**Message Description:** LOGID\_EVENT\_TWO\_F\_AUTH\_CODE\_SENDTO

**Message Meaning:** Two-factor authentication code sent

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 38412 - LOGID\_EVENT\_TOKEN\_CODE\_SENDTO

**Message ID:** 38412

**Message Description:** LOGID\_EVENT\_TOKEN\_CODE\_SENDTO

**Message Meaning:** Token activation code sent

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 38420 - LOGID\_EVENT\_HTTPS\_CONNECTION

**Message ID:** 38420

**Message Description:** LOGID\_EVENT\_HTTPS\_CONNECTION

**Message Meaning:** HTTPS connection

**Type:** Event

**Category:** SYSTEM

**Severity:** Information



Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256
remote	IP Address of the PPP Remote end	ip	39

## 38656 - LOGID\_EVENT\_RAD\_RPT\_PROTO\_ERROR

**Message ID:** 38656

**Message Description:** LOGID\_EVENT\_RAD\_RPT\_PROTO\_ERROR

**Message Meaning:** RADIUS protocol error summary

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
count	Number of Packets	uint32	10
duration	Duration	uint32	10

## 38657 - LOGID\_EVENT\_RAD\_RPT\_PROF\_NOT\_FOUND

**Message ID:** 38657

**Message Description:** LOGID\_EVENT\_RAD\_RPT\_PROF\_NOT\_FOUND

**Message Meaning:** RADIUS profile not found summary

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
count	Number of Packets	uint32	10
duration	Duration	uint32	10

## 38658 - LOGID\_EVENT\_RAD\_RPT\_CTX\_NOT\_FOUND

**Message ID:** 38658

**Message Description:** LOGID\_EVENT\_RAD\_RPT\_CTX\_NOT\_FOUND

**Message Meaning:** RADIUS profile CTX not found summary

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
count	Number of Packets	uint32	10
duration	Duration	uint32	10

## 38659 - LOGID\_EVENT\_RAD\_RPT\_ACCT\_STOP\_MISSED

**Message ID:** 38659

**Message Description:** LOGID\_EVENT\_RAD\_RPT\_ACCT\_STOP\_MISSED

**Message Meaning:** RADIUS accounting stop message missing summary

**Type:** Event

**Category:** USER**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
count	Number of Packets	uint32	10
duration	Duration	uint32	10

## 38660 - LOGID\_EVENT\_RAD\_RPT\_ACCT\_EVENT

**Message ID:** 38660**Message Description:** LOGID\_EVENT\_RAD\_RPT\_ACCT\_EVENT**Message Meaning:** RADIUS accounting event summary**Type:** Event**Category:** USER**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
count	Number of Packets	uint32	10
duration	Duration	uint32	10

## 38661 - LOGID\_EVENT\_RAD\_RPT\_OTHER

**Message ID:** 38661

**Message Description:** LOGID\_EVENT\_RAD\_RPT\_OTHER

**Message Meaning:** RADIUS endpoint block event or other event summary

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
count	Number of Packets	uint32	10
duration	Duration	uint32	10

## 38662 - LOGID\_EVENT\_RAD\_STAT\_PROTO\_ERROR

**Message ID:** 38662

**Message Description:** LOGID\_EVENT\_RAD\_STAT\_PROTO\_ERROR

**Message Meaning:** RADIUS accounting protocol error

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
carrier_ep	The FortiOS Carrier end-point identification	string	64
rsso_key	RADIUS SSO attribute value	string	64
acct_stat	Accounting state (RADIUS)	string	14

## 38663 - LOGID\_EVENT\_RAD\_STAT\_PROF\_NOT\_FOUND

**Message ID:** 38663

**Message Description:** LOGID\_EVENT\_RAD\_STAT\_PROF\_NOT\_FOUND

**Message Meaning:** RADIUS accounting profile not found

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
carrier_ep	The FortiOS Carrier end-point identification	string	64
rsso_key	RADIUS SSO attribute value	string	64
acct_stat	Accounting state (RADIUS)	string	14

**38665 - LOGID\_EVENT\_RAD\_STAT\_ACCT\_STOP\_MISSED****Message ID:** 38665**Message Description:** LOGID\_EVENT\_RAD\_STAT\_ACCT\_STOP\_MISSED**Message Meaning:** RADIUS accounting stop message missing**Type:** Event**Category:** USER**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
carrier_ep	The FortiOS Carrier end-point identification	string	64
rsso_key	RADIUS SSO attribute value	string	64
acct_stat	Accounting state (RADIUS)	string	14

## 38666 - LOGID\_EVENT\_RAD\_STAT\_ACCT\_EVENT

**Message ID:** 38666

**Message Description:** LOGID\_EVENT\_RAD\_STAT\_ACCT\_EVENT

**Message Meaning:** RADIUS accounting event

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16



Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
srcip	Source IP	ip	39
carrier_ep	The FortiOS Carrier end-point identification	string	64
rsso_key	RADIUS SSO attribute value	string	64
acct_stat	Accounting state (RADIUS)	string	14

## 38667 - LOGID\_EVENT\_RAD\_STAT\_OTHER

**Message ID:** 38667

**Message Description:** LOGID\_EVENT\_RAD\_STAT\_OTHER

**Message Meaning:** RADIUS other accounting event

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
srcip	Source IP	ip	39
reason	Reason	string	256
count	Number of Packets	uint32	10
carrier_ep	The FortiOS Carrier end-point identification	string	64
rsso_key	RADIUS SSO attribute value	string	64
acct_stat	Accounting state (RADIUS)	string	14

## 38668 - LOGID\_EVENT\_RAD\_STAT\_EP\_BLK

**Message ID:** 38668

**Message Description:** LOGID\_EVENT\_RAD\_STAT\_EP\_BLK

**Message Meaning:** RADIUS endpoint block event

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
carrier_ep	The FortiOS Carrier end-point identification	string	64

Log Field Name	Description	Data Type	Length
rsso_key	RADIUS SSO attribute value	string	64
acct_stat	Accounting state (RADIUS)	string	14

## 39424 - LOG\_ID\_EVENT\_SSL\_VPN\_USER\_TUNNEL\_UP

**Message ID:** 39424

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_USER\_TUNNEL\_UP

**Message Meaning:** SSL VPN tunnel up

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39425 - LOG\_ID\_EVENT\_SSL\_VPN\_USER\_TUNNEL\_DOWN

**Message ID:** 39425

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_USER\_TUNNEL\_DOWN

**Message Meaning:** SSL VPN tunnel down

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
duration	Duration	uint32	10
sentbyte	Bytes Sent	uint64	20
rcvdbyte	Received Bytes	uint64	20
dst_host	Destination Host	string	64

## 39426 - LOG\_ID\_EVENT\_SSL\_VPN\_USER\_SSL\_LOGIN\_FAIL

**Message ID:** 39426

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_USER\_SSL\_LOGIN\_FAIL

**Message Meaning:** SSL VPN login fail

**Type:** Event

**Category:** VPN

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39936 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_WEB\_TUNNEL\_STATS

**Message ID:** 39936

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_WEB\_TUNNEL\_STATS

**Message Meaning:** SSL VPN statistics

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
duration	Duration	uint32	10
sentbyte	Bytes Sent	uint64	20
rcvdbyte	Received Bytes	uint64	20
nextstat	Time interval in seconds for the next statistics	uint32	10
dst_host	Destination Host	string	64

## 39937 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_WEBAPP\_DENY

**Message ID:** 39937

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_WEBAPP\_DENY

**Message Meaning:** SSL VPN deny**Type:** Event**Category:** VPN**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39938 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_WEBAPP\_PASS

**Message ID:** 39938**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_WEBAPP\_PASS**Message Meaning:** SSL VPN pass**Type:** Event**Category:** VPN**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39939 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_WEBAPP\_TIMEOUT

**Message ID:** 39939

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_WEBAPP\_TIMEOUT

**Message Meaning:** SSL VPN timeout

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10



Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39940 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_WEBAPP\_CLOSE

**Message ID:** 39940

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_WEBAPP\_CLOSE

**Message Meaning:** SSL VPN close

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39941 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_SYS\_BUSY

**Message ID:** 39941

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_SYS\_BUSY

**Message Meaning:** SSL VPN system busy

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39942 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_CERT\_OK

**Message ID:** 39942

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_CERT\_OK

**Message Meaning:** SSL VPN certificate OK

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39943 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_NEW\_CON

**Message ID:** 39943

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_NEW\_CON

**Message Meaning:** SSL VPN new connection

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39944 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_ALERT

**Message ID:** 39944

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_ALERT

**Message Meaning:** SSL VPN alert

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64
desc	Description	string	128

## 39945 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_EXIT\_FAIL

**Message ID:** 39945

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_EXIT\_FAIL

**Message Meaning:** SSL VPN exit fail

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39946 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_EXIT\_ERR

**Message ID:** 39946

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_EXIT\_ERR

**Message Meaning:** SSL VPN exit error

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39947 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_TUNNEL\_UP

**Message ID:** 39947

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_TUNNEL\_UP

**Message Meaning:** SSL VPN tunnel up

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32



Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39948 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_TUNNEL\_DOWN

**Message ID:** 39948

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_TUNNEL\_DOWN

**Message Meaning:** SSL VPN tunnel down

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
duration	Duration	uint32	10
sentbyte	Bytes Sent	uint64	20
rcvdbyte	Received Bytes	uint64	20
dst_host	Destination Host	string	64

## 39949 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_TUNNEL\_STATS

**Message ID:** 39949

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_TUNNEL\_STATS

**Message Meaning:** SSL VPN statistics

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
duration	Duration	uint32	10
sentbyte	Bytes Sent	uint64	20
rcvdbyte	Received Bytes	uint64	20
nextstat	Time interval in seconds for the next statistics	uint32	10
dst_host	Destination Host	string	64

## 39950 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_TUNNEL\_UNKNOWN\_TAG

**Message ID:** 39950

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_TUNNEL\_UNKNOWN\_TAG

**Message Meaning:** SSL VPN unknown tag

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39951 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_TUNNEL\_ERROR

**Message ID:** 39951

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_TUNNEL\_ERROR

**Message Meaning:** SSL VPN tunnel error

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39952 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_ENTER\_CONSERVE\_MODE

**Message ID:** 39952

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_ENTER\_CONSERVE\_MODE

**Message Meaning:** SSL VPN enter conserve mode

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 39953 - LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_LEAVE\_CONSERVE\_MODE

**Message ID:** 39953

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SESSION\_LEAVE\_CONSERVE\_MODE

**Message Meaning:** SSL VPN leave conserve mode

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096
reason	Reason	string	256
dst_host	Destination Host	string	64

## 40001 - LOG\_ID\_PPTP\_TUNNEL\_UP

**Message ID:** 40001

**Message Description:** LOG\_ID\_PPTP\_TUNNEL\_UP

**Message Meaning:** PPTP tunnel up

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
tunnelip	IPsec VPN tunnel IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096

## 40002 - LOG\_ID\_PPTP\_TUNNEL\_DOWN

**Message ID:** 40002

**Message Description:** LOG\_ID\_PPTP\_TUNNEL\_DOWN

**Message Meaning:** PPTP tunnel down

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096



Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
tunnelip	IPsec VPN tunnel IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096

## 40003 - LOG\_ID\_PPTP\_TUNNEL\_STAT

**Message ID:** 40003

**Message Description:** LOG\_ID\_PPTP\_TUNNEL\_STAT

**Message Meaning:** PPTP tunnel status

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10

Log Field Name	Description	Data Type	Length
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
tunnelip	IPsec VPN tunnel IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096

## 40014 - LOG\_ID\_PPTP\_REACH\_MAX\_CON

**Message ID:** 40014

**Message Description:** LOG\_ID\_PPTP\_REACH\_MAX\_CON

**Message Meaning:** PPTP client connection limit reached

**Type:** Event

**Category:** VPN

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23

## 40017 - LOG\_ID\_L2TPD\_CLIENT\_CON\_FAIL

**Message ID:** 40017

**Message Description:** LOG\_ID\_L2TPD\_CLIENT\_CON\_FAIL

**Message Meaning:** L2TP client connection failed

**Type:** Event

**Category:** VPN

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23
reason	Reason	string	256

## 40019 - LOG\_ID\_L2TPD\_CLIENT\_DISCON

**Message ID:** 40019

**Message Description:** LOG\_ID\_L2TPD\_CLIENT\_DISCON

**Message Meaning:** L2TP client disconnected

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23

## 40021 - LOG\_ID\_PPTP\_NOT\_CONIG

**Message ID:** 40021

**Message Description:** LOG\_ID\_PPTP\_NOT\_CONIG

**Message Meaning:** PPTP not configured in VDOM

**Type:** Event

**Category:** VPN

**Severity:** Debug

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23

## 40022 - LOG\_ID\_PPTP\_NO\_IP\_AVAIL

**Message ID:** 40022

**Message Description:** LOG\_ID\_PPTP\_NO\_IP\_AVAIL

**Message Meaning:** PPTP IP addresses unavailable

**Type:** Event

**Category:** VPN

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23

## 40024 - LOG\_ID\_PPTP\_OUT\_MEM

**Message ID:** 40024

**Message Description:** LOG\_ID\_PPTP\_OUT\_MEM

**Message Meaning:** PPTP config list insufficient memory

**Type:** Event

**Category:** VPN

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23

## 40034 - LOG\_ID\_PPTP\_START

**Message ID:** 40034

**Message Description:** LOG\_ID\_PPTP\_START

**Message Meaning:** PPTP daemon started

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23

## 40035 - LOG\_ID\_PPTP\_START\_FAIL

**Message ID:** 40035

**Message Description:** LOG\_ID\_PPTP\_START\_FAIL

**Message Meaning:** PPTP daemon failed to start

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23
reason	Reason	string	256

## 40036 - LOG\_ID\_PPTP\_EXIT

**Message ID:** 40036

**Message Description:** LOG\_ID\_PPTP\_EXIT

**Message Meaning:** PPTP daemon exited

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23



## 40037 - LOG\_ID\_PPTPD\_SVR\_DISCON

**Message ID:** 40037

**Message Description:** LOG\_ID\_PPTPD\_SVR\_DISCON

**Message Meaning:** PPTP daemon disconnected

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23
reason	Reason	string	256

## 40038 - LOG\_ID\_PPTPD\_CLIENT\_CON

**Message ID:** 40038

**Message Description:** LOG\_ID\_PPTPD\_CLIENT\_CON

**Message Meaning:** PPTP client connected

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23

## 40039 - LOG\_ID\_PPTPD\_CLIENT\_DISCON

**Message ID:** 40039

**Message Description:** LOG\_ID\_PPTPD\_CLIENT\_DISCON

**Message Meaning:** PPTP client disconnected

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23

## 40101 - LOG\_ID\_L2TP\_TUNNEL\_UP

**Message ID:** 40101

**Message Description:** LOG\_ID\_L2TP\_TUNNEL\_UP

**Message Meaning:** L2TP tunnel up

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64

Log Field Name	Description	Data Type	Length
remip	IPsec VPN remote gateway IP address	ip	39
tunnelip	IPsec VPN tunnel IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096

## 40102 - LOG\_ID\_L2TP\_TUNNEL\_DOWN

**Message ID:** 40102

**Message Description:** LOG\_ID\_L2TP\_TUNNEL\_DOWN

**Message Meaning:** L2TP tunnel down

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
tunnelip	IPsec VPN tunnel IP address	ip	39

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096

## 40103 - LOG\_ID\_L2TP\_TUNNEL\_STAT

**Message ID:** 40103

**Message Description:** LOG\_ID\_L2TP\_TUNNEL\_STAT

**Message Meaning:** L2TP tunnel status

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
tunnelid	IPsec VPN tunnel ID	uint32	10
tunneltype	IPsec VPN tunnel type	string	64
remip	IPsec VPN remote gateway IP address	ip	39
tunnelip	IPsec VPN tunnel IP address	ip	39
user	User name of authenticated user	string	256
group	User group Name	string	64
msg	Log Message	string	4096

## 40114 - LOG\_ID\_L2TPD\_START

**Message ID:** 40114

**Message Description:** LOG\_ID\_L2TPD\_START

**Message Meaning:** L2TP daemon started

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23

## 40115 - LOG\_ID\_L2TPD\_EXIT

**Message ID:** 40115

**Message Description:** LOG\_ID\_L2TPD\_EXIT

**Message Meaning:** L2TP daemon exited

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23

## 40118 - LOG\_ID\_L2TPD\_CLIENT\_CON

**Message ID:** 40118

**Message Description:** LOG\_ID\_L2TPD\_CLIENT\_CON

**Message Meaning:** L2TP client connected

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23

## 40704 - LOG\_ID\_EVENT\_SYS\_PERF

**Message ID:** 40704

**Message Description:** LOG\_ID\_EVENT\_SYS\_PERF

**Message Meaning:** System performance statistics

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096



Log Field Name	Description	Data Type	Length
name	Display Name of the Connection	string	128
sn	Serial Number	string	64
cpu	CPU Usage	uint8	3
mem	Memory Usage	uint8	3
totalsession	Total Number of Sessions	uint32	10
disk	Disk Usage	uint8	3
bandwidth	Bandwidth	string	42
setuprate	Session Setup Rate	uint64	20
disklograte	Disk Log Rate	uint64	20
fazlograte	FortiAnalyzer Logging Rate	uint64	20
freediskstorage		uint32	10
sysuptime		uint32	10
waninfo		string	512



This log message is only sent to remote FortiAnalyzer and memory, but not to disk.

## 40705 - LOG\_ID\_EVENT\_SYS\_CPU\_USAGE

**Message ID:** 40705

**Message Description:** LOG\_ID\_EVENT\_SYS\_CPU\_USAGE

**Message Meaning:** CPU usage statistics

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
cpu	CPU Usage	uint8	3

## 40706 - LOG\_ID\_EVENT\_SYS\_BROKEN\_SYMBOLIC\_LINK

**Message ID:** 40706

**Message Description:** LOG\_ID\_EVENT\_SYS\_BROKEN\_SYMBOLIC\_LINK

**Message Meaning:** Delete broken symbolic link

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 40960 - LOGID\_EVENT\_WAD\_WEBPROXY\_FWD\_SRV\_ERROR

**Message ID:** 40960

**Message Description:** LOGID\_EVENT\_WAD\_WEBPROXY\_FWD\_SRV\_ERROR

**Message Meaning:** Web proxy forward server error

**Type:** Event

**Category:** WAD

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
fwserver_name	WAD forward server name	string	32
addr_type	Address Type	string	4
ip		ip	39
fqdn	Fully Qualified Domain Name	string	256
port	Port Number	uint16	5
msg	Log Message	string	4096

## 41000 - LOG\_ID\_UPD\_FGT\_SUCC

**Message ID:** 41000

**Message Description:** LOG\_ID\_UPD\_FGT\_SUCC

**Message Meaning:** FortiGate update succeeded

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096

## 41001 - LOG\_ID\_UPD\_FGT\_FAIL

**Message ID:** 41001**Message Description:** LOG\_ID\_UPD\_FGT\_FAIL**Message Meaning:** FortiGate update failed**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096

## 41002 - LOG\_ID\_UPD\_SRC\_VIS

**Message ID:** 41002

**Message Description:** LOG\_ID\_UPD\_SRC\_VIS

**Message Meaning:** Source visibility signature package updated

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096

## 41006 - LOG\_ID\_UPD\_FSA\_VIRDB

**Message ID:** 41006

**Message Description:** LOG\_ID\_UPD\_FSA\_VIRDB

**Message Meaning:** FortiSandbox AV database updated

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
version	Version	string	64

## 41009 - LOG\_ID\_UPD\_DB\_SIGN\_INVALID

**Message ID:** 41009

**Message Description:** LOG\_ID\_UPD\_DB\_SIGN\_INVALID

**Message Meaning:** FortiGate database signature invalid

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 41984 - LOG\_ID\_EVENT\_VPN\_CERT\_LOAD

**Message ID:** 41984

**Message Description:** LOG\_ID\_EVENT\_VPN\_CERT\_LOAD

**Message Meaning:** Certificate loaded

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
name	Display Name of the Connection	string	128
cert-type	Certification type	string	6

## 41985 - LOG\_ID\_EVENT\_VPN\_CERT\_REMOVAL

**Message ID:** 41985

**Message Description:** LOG\_ID\_EVENT\_VPN\_CERT\_REMOVAL

**Message Meaning:** Certificate removed

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096



Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
user	User name of authenticated user	string	256
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
name	Display Name of the Connection	string	128
cert-type	Certification type	string	6

## 41986 - LOG\_ID\_EVENT\_VPN\_CERT\_REGEN

**Message ID:** 41986

**Message Description:** LOG\_ID\_EVENT\_VPN\_CERT\_REGEN

**Message Meaning:** Certificate regenerated

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
status	Status	string	23
ui	User Interface	string	64
name	Display Name of the Connection	string	128
cert-type	Certification type	string	6

## 41987 - LOG\_ID\_EVENT\_VPN\_CERT\_UPDATE

**Message ID:** 41987

**Message Description:** LOG\_ID\_EVENT\_VPN\_CERT\_UPDATE

**Message Meaning:** Certificate updated

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23
reason	Reason	string	256
name	Display Name of the Connection	string	128
cert-type	Certification type	string	6
method	Method	string	64

## 41988 - LOG\_ID\_EVENT\_SSL\_VPN\_SETTING\_UPDATE

**Message ID:** 41988

**Message Description:** LOG\_ID\_EVENT\_SSL\_VPN\_SETTING\_UPDATE

**Message Meaning:** SSL setting changed

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
msg	Log Message	string	4096
ui	User Interface	string	64

## 41989 - LOG\_ID\_EVENT\_VPN\_CERT\_ERR

**Message ID:** 41989

**Message Description:** LOG\_ID\_EVENT\_VPN\_CERT\_ERR

**Message Meaning:** Certificate error

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23
name	Display Name of the Connection	string	128
cert-type	Certification type	string	6
method	Method	string	64

## 41990 - LOG\_ID\_EVENT\_VPN\_CERT\_UPDATE\_FAILED

**Message ID:** 41990

**Message Description:** LOG\_ID\_EVENT\_VPN\_CERT\_UPDATE\_FAILED

**Message Meaning:** Certificate update failed

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23
reason	Reason	string	256
name	Display Name of the Connection	string	128
cert-type	Certification type	string	6
method	Method	string	64

## 41991 - LOG\_ID\_EVENT\_VPN\_CERT\_EXPORT

**Message ID:** 41991

**Message Description:** LOG\_ID\_EVENT\_VPN\_CERT\_EXPORT

**Message Meaning:** Certificate exported

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
user	User name of authenticated user	string	256
msg	Log Message	string	4096
status	Status	string	23
ui	User Interface	string	64
name	Display Name of the Connection	string	128
cert-type	Certification type	string	6

## 41992 - LOG\_ID\_EVENT\_VPN\_CERT\_CRL\_EXPIRED

**Message ID:** 41992

**Message Description:** LOG\_ID\_EVENT\_VPN\_CERT\_CRL\_EXPIRED

**Message Meaning:** CRL certificate file is expired

**Type:** Event

**Category:** VPN

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
status	Status	string	23
name	Display Name of the Connection	string	128
cert-type	Certification type	string	6
method	Method	string	64

## 42201 - LOG\_ID\_NETX\_VMX\_ATTACH

**Message ID:** 42201

**Message Description:** LOG\_ID\_NETX\_VMX\_ATTACH

**Message Meaning:** VMX instance successfully attached

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 42202 - LOG\_ID\_NETX\_VMX\_DETACH

**Message ID:** 42202

**Message Description:** LOG\_ID\_NETX\_VMX\_DETACH

**Message Meaning:** VMX instance successfully detached

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 42203 - LOG\_ID\_NETX\_VMX\_DENIED

**Message ID:** 42203

**Message Description:** LOG\_ID\_NETX\_VMX\_DENIED

**Message Meaning:** VMX instance successfully denied

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16



Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 43008 - LOG\_ID\_EVENT\_AUTH\_SUCCESS

**Message ID:** 43008

**Message Description:** LOG\_ID\_EVENT\_AUTH\_SUCCESS

**Message Meaning:** Authentication success

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
policyid	Policy ID	uint32	10
interface	Interface	string	32
group	User group Name	string	64

## 43009 - LOG\_ID\_EVENT\_AUTH\_FAILED

**Message ID:** 43009

**Message Description:** LOG\_ID\_EVENT\_AUTH\_FAILED

**Message Meaning:** Authentication failed

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256

Log Field Name	Description	Data Type	Length
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
policyid	Policy ID	uint32	10
interface	Interface	string	32
group	User group Name	string	64

## 43010 - LOG\_ID\_EVENT\_AUTH\_LOCKOUT

**Message ID:** 43010

**Message Description:** LOG\_ID\_EVENT\_AUTH\_LOCKOUT

**Message Meaning:** Authentication lockout

**Type:** Event

**Category:** USER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
policyid	Policy ID	uint32	10
interface	Interface	string	32
group	User group Name	string	64

## 43011 - LOG\_ID\_EVENT\_AUTH\_TIME\_OUT

**Message ID:** 43011

**Message Description:** LOG\_ID\_EVENT\_AUTH\_TIME\_OUT

**Message Meaning:** Authentication timed out

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
policyid	Policy ID	uint32	10
interface	Interface	string	32
group	User group Name	string	64
authserver	Remote Authentication server	string	64

## 43014 - LOG\_ID\_EVENT\_AUTH\_FSAE\_LOGON

**Message ID:** 43014

**Message Description:** LOG\_ID\_EVENT\_AUTH\_FSAE\_LOGON

**Message Meaning:** FSSO logon authentication status

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096
srcip	Source IP	ip	39
server	AD server FQDN or IP	string	64

## 43015 - LOG\_ID\_EVENT\_AUTH\_FSAE\_LOGOFF

**Message ID:** 43015

**Message Description:** LOG\_ID\_EVENT\_AUTH\_FSAE\_LOGOFF

**Message Meaning:** FSSO log off authentication status

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
srcip	Source IP	ip	39
server	AD server FQDN or IP	string	64

## 43016 - LOG\_ID\_EVENT\_AUTH\_NTLM\_AUTH\_SUCCESS

**Message ID:** 43016

**Message Description:** LOG\_ID\_EVENT\_AUTH\_NTLM\_AUTH\_SUCCESS

**Message Meaning:** NTLM authentication successful

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256

Log Field Name	Description	Data Type	Length
dstip	Destination IP	ip	39
policyid	Policy ID	uint32	10
group	User group Name	string	64
adgroup	AD Group Name of FSSO user	string	128

## 43017 - LOG\_ID\_EVENT\_AUTH\_NTLM\_AUTH\_FAIL

**Message ID:** 43017

**Message Description:** LOG\_ID\_EVENT\_AUTH\_NTLM\_AUTH\_FAIL

**Message Meaning:** NTLM authentication failed

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39



Log Field Name	Description	Data Type	Length
reason	Reason	string	256
dstip	Destination IP	ip	39
policyid	Policy ID	uint32	10
group	User group Name	string	64
adgroup	AD Group Name of FSSO user	string	128

## 43018 - LOG\_ID\_EVENT\_AUTH\_FGOVRD\_FAIL

**Message ID:** 43018

**Message Description:** LOG\_ID\_EVENT\_AUTH\_FGOVRD\_FAIL

**Message Meaning:** FortiGuard override failed

**Type:** Event

**Category:** USER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
initiator	Original login user name for Fortiguard override	string	64

## 43020 - LOG\_ID\_EVENT\_AUTH\_FGOVRD\_SUCCESS

**Message ID:** 43020

**Message Description:** LOG\_ID\_EVENT\_AUTH\_FGOVRD\_SUCCESS

**Message Meaning:** FortiGuard override successful

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
initiator	Original login user name for Fortiguard override	string	64
scope	FortiGuard Override Scope	string	16
expiry	FortiGuard override expiry timestamp	string	64
oldwprof	Old Web Filter Profile	string	64

## 43025 - LOG\_ID\_EVENT\_AUTH\_PROXY\_SUCCESS

**Message ID:** 43025

**Message Description:** LOG\_ID\_EVENT\_AUTH\_PROXY\_SUCCESS

**Message Meaning:** Explicit proxy authentication successful

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
group	User group Name	string	64
authid		string	36

## 43026 - LOG\_ID\_EVENT\_AUTH\_PROXY\_FAILED

**Message ID:** 43026

**Message Description:** LOG\_ID\_EVENT\_AUTH\_PROXY\_FAILED

**Message Meaning:** Explicit proxy authentication failed

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
group	User group Name	string	64
authid		string	36

## 43027 - LOG\_ID\_EVENT\_AUTH\_PROXY\_TIME\_OUT

**Message ID:** 43027**Message Description:** LOG\_ID\_EVENT\_AUTH\_PROXY\_TIME\_OUT**Message Meaning:** Explicit proxy authentication timed out**Type:** Event**Category:** USER**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
group	User group Name	string	64

## 43028 - LOG\_ID\_EVENT\_AUTH\_PROXY\_GROUP\_INFO\_FAILED

**Message ID:** 43028

**Message Description:** LOG\_ID\_EVENT\_AUTH\_PROXY\_GROUP\_INFO\_FAILED

**Message Meaning:** Explicit proxy user group query failed

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
group	User group Name	string	64
authid		string	36

## 43029 - LOG\_ID\_EVENT\_AUTH\_WARNING\_SUCCESS

**Message ID:** 43029

**Message Description:** LOG\_ID\_EVENT\_AUTH\_WARNING\_SUCCESS

**Message Meaning:** FortiGuard authentication override successful

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
initiator	Original login user name for Fortiguard override	string	64
scope	FortiGuard Override Scope	string	16
expiry	FortiGuard override expiry timestamp	string	64
oldwprof	Old Web Filter Profile	string	64
category	Log category	uint32	10

## 43030 - LOG\_ID\_EVENT\_AUTH\_WARNING\_TBL\_FULL

**Message ID:** 43030

**Message Description:** LOG\_ID\_EVENT\_AUTH\_WARNING\_TBL\_FULL

**Message Meaning:** FortiGuard authentication override failed

**Type:** Event

**Category:** USER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
initiator	Original login user name for Fortiguard override	string	64

## 43032 - LOG\_ID\_EVENT\_AUTH\_PROXY\_USER\_LIMIT\_REACHED

**Message ID:** 43032

**Message Description:** LOG\_ID\_EVENT\_AUTH\_PROXY\_USER\_LIMIT\_REACHED

**Message Meaning:** Explicit proxy authentication user limit reached

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20



Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
group	User group Name	string	64
authid		string	36

## 43033 - LOG\_ID\_EVENT\_AUTH\_PROXY\_MULTIPLE\_LOGIN

**Message ID:** 43033

**Message Description:** LOG\_ID\_EVENT\_AUTH\_PROXY\_MULTIPLE\_LOGIN

**Message Meaning:** Explicit proxy authentication user concurrent check failed

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
group	User group Name	string	64
authid		string	36

## 43034 - LOG\_ID\_EVENT\_AUTH\_PROXY\_NO\_RESP

**Message ID:** 43034

**Message Description:** LOG\_ID\_EVENT\_AUTH\_PROXY\_NO\_RESP

**Message Meaning:** Explicit proxy authentication no response

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
dstip	Destination IP	ip	39
policyid	Policy ID	uint32	10
url	URL	string	512
agent	SNMP agent	string	64

## 43037 - LOG\_ID\_EVENT\_AUTH\_IPV4\_FLUSH

**Message ID:** 43037

**Message Description:** LOG\_ID\_EVENT\_AUTH\_IPV4\_FLUSH

**Message Meaning:** Authentication IPv4 logon flush

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 43038 - LOG\_ID\_EVENT\_AUTH\_IPV6\_FLUSH

**Message ID:** 43038

**Message Description:** LOG\_ID\_EVENT\_AUTH\_IPV6\_FLUSH

**Message Meaning:** Authentication IPv6 logon flush

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096

## 43039 - LOG\_ID\_EVENT\_AUTH\_LOGON

**Message ID:** 43039

**Message Description:** LOG\_ID\_EVENT\_AUTH\_LOGON

**Message Meaning:** Authentication logon

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64

## 43040 - LOG\_ID\_EVENT\_AUTH\_LOGOUT

**Message ID:** 43040

**Message Description:** LOG\_ID\_EVENT\_AUTH\_LOGOUT

**Message Meaning:** Authentication logout

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
authserver	Remote Authentication server	string	64

**43041 - LOG\_ID\_EVENT\_AUTH\_DISCLAIMER\_ACCEPT****Message ID:** 43041**Message Description:** LOG\_ID\_EVENT\_AUTH\_DISCLAIMER\_ACCEPT**Message Meaning:** Disclaimer accepted**Type:** Event**Category:** USER**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
policyid	Policy ID	uint32	10
interface	Interface	string	32
group	User group Name	string	64

## 43042 - LOG\_ID\_EVENT\_AUTH\_DISCLAIMER\_DECLINE

**Message ID:** 43042

**Message Description:** LOG\_ID\_EVENT\_AUTH\_DISCLAIMER\_DECLINE

**Message Meaning:** Disclaimer declined

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
policyid	Policy ID	uint32	10
interface	Interface	string	32
group	User group Name	string	64

## 43043 - LOG\_ID\_EVENT\_AUTH\_EMAIL\_COLLECTING\_SUCCESS

**Message ID:** 43043

**Message Description:** LOG\_ID\_EVENT\_AUTH\_EMAIL\_COLLECTING\_SUCCESS

**Message Meaning:** Email collecting succeeded

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10



Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
policyid	Policy ID	uint32	10
interface	Interface	string	32
group	User group Name	string	64

## 43044 - LOG\_ID\_EVENT\_AUTH\_EMAIL\_COLLECTING\_FAIL

**Message ID:** 43044

**Message Description:** LOG\_ID\_EVENT\_AUTH\_EMAIL\_COLLECTING\_FAIL

**Message Meaning:** Email collecting failed

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
authproto	The protocol that initiated the authentication	string	512
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
srcip	Source IP	ip	39
reason	Reason	string	256
dstip	Destination IP	ip	39
policyid	Policy ID	uint32	10
interface	Interface	string	32
group	User group Name	string	64

## 43045 - LOG\_ID\_EVENT\_AUTH\_8021X\_SUCCESS

**Message ID:** 43045

**Message Description:** LOG\_ID\_EVENT\_AUTH\_8021X\_SUCCESS

**Message Meaning:** 802.1x authentication succeeded

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256
interface	Interface	string	32
stamac	The MAC address of wifi station	string	17

## 43046 - LOG\_ID\_EVENT\_AUTH\_8021X\_FAIL

**Message ID:** 43046

**Message Description:** LOG\_ID\_EVENT\_AUTH\_8021X\_FAIL

**Message Meaning:** 802.1x authentication failed

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
reason	Reason	string	256
interface	Interface	string	32
stamac	The MAC address of wifi station	string	17

## 43050 - LOG\_ID\_EVENT\_AUTH\_FSAE\_CONNECT

**Message ID:** 43050

**Message Description:** LOG\_ID\_EVENT\_AUTH\_FSAE\_CONNECT

**Message Meaning:** FSSO server connected

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
server	AD server FQDN or IP	string	64

## 43051 - LOG\_ID\_EVENT\_AUTH\_FSAE\_DISCONNECT

**Message ID:** 43051

**Message Description:** LOG\_ID\_EVENT\_AUTH\_FSAE\_DISCONNECT

**Message Meaning:** FSSO server disconnected

**Type:** Event

**Category:** USER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
server	AD server FQDN or IP	string	64

## 43520 - LOG\_ID\_EVENT\_WIRELESS\_SYS

**Message ID:** 43520

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_SYS

**Message Meaning:** Wireless system activity

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 43521 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE

**Message ID:** 43521

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE

**Message Meaning:** Rogue AP activity

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36

Log Field Name	Description	Data Type	Length
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43522 - LOG\_ID\_EVENT\_WIRELESS\_WTP

**Message ID:** 43522

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP

**Message Meaning:** Physical AP activity

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64



Log Field Name	Description	Data Type	Length
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43524 - LOG\_ID\_EVENT\_WIRELESS\_STA

**Message ID:** 43524

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA

**Message Meaning:** Wireless client activity

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40

Log Field Name	Description	Data Type	Length
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43525 - LOG\_ID\_EVENT\_WIRELESS\_ONWIRE

**Message ID:** 43525

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ONWIRE

**Message Meaning:** Rogue AP on wire

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43526 - LOG\_ID\_EVENT\_WIRELESS\_WTPR

**Message ID:** 43526

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR

**Message Meaning:** Physical AP radio activity

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmamode		string	10
operdrmmamode		string	10

## 43527 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_CFG

**Message ID:** 43527

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_CFG

**Message Meaning:** Rogue AP status configured

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43528 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_ERROR

**Message ID:** 43528

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_ERROR

**Message Meaning:** Physical AP radio error activity

**Type:** Event

**Category:** WIRELESS

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmode		string	10
operdrmmode		string	10

## 43529 - LOG\_ID\_EVENT\_WIRELESS\_CLB

**Message ID:** 43529**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_CLB

**Message Meaning:** Wireless client load balancing

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
stamac	The MAC address of wifi station	string	17
stacount	The count of wifi stations	uint32	10
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36

## 43530 - LOG\_ID\_EVENT\_WIRELESS\_WIDS\_WL\_BRIDGE

**Message ID:** 43530

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WIDS\_WL\_BRIDGE

**Message Meaning:** Wireless bridge intrusion detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
bssid	Basic service set ID	string	17
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
threattype	WIDS threat type	string	64
rsssi	The value of Received signal strength indicator	uint8	3
frametype	Frame Type	string	32
ds	Direction with distribution system	string	8
seq	Sequence	string	512
encrypt	The packet is encrypted or not	uint8	3
tamac	The MAC address of Transmitter. If none, then Receiver	string	17

**43531 - LOG\_ID\_EVENT\_WIRELESS\_WIDS\_BR\_DEAUTH****Message ID:** 43531



**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WIDS\_BR\_DEAUTH

**Message Meaning:** Wireless broadcasting deauthentication detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
bssid	Basic service set ID	string	17
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
threattype	WIDS threat type	string	64
rsi	The value of Received signal strength indicator	uint8	3
frametype	Frame Type	string	32
ds	Direction with distribution system	string	8
seq	Sequence	string	512
encrypt	The packet is encrypted or not	uint8	3
tamac	The MAC address of Transmitter. If none, then Receiver	string	17

## 43532 - LOG\_ID\_EVENT\_WIRELESS\_WIDS\_NL\_PBRESP

**Message ID:** 43532

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WIDS\_NL\_PBRESP

**Message Meaning:** Wireless null SSID probe response detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
bssid	Basic service set ID	string	17
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
threatype	WIDS threat type	string	64
rss	The value of Received signal strength indicator	uint8	3
frametype	Frame Type	string	32

Log Field Name	Description	Data Type	Length
ds	Direction with distribution system	string	8
seq	Sequence	string	512
encrypt	The packet is encrypted or not	uint8	3
tamac	The MAC address of Transmitter. If none, then Receiver	string	17

## 43533 - LOG\_ID\_EVENT\_WIRELESS\_WIDS\_MAC\_OUI

**Message ID:** 43533

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WIDS\_MAC\_OUI

**Message Meaning:** Wireless invalid MAC OUI detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
bssid	Basic service set ID	string	17
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
live	Time in seconds	uint32	10

Log Field Name	Description	Data Type	Length
age	Time in seconds - time passed since last seen	uint32	10
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
threattype	WIDS threat type	string	64
rsssi	The value of Received signal strength indicator	uint8	3
frametype	Frame Type	string	32
ds	Direction with distribution system	string	8
seq	Sequence	string	512
encrypt	The packet is encrypted or not	uint8	3
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
invalidmac	Detected MAC address with invalid OUI	string	17

## 43534 - LOG\_ID\_EVENT\_WIRELESS\_WIDS\_LONG\_DUR

**Message ID:** 43534

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WIDS\_LONG\_DUR

**Message Meaning:** Wireless long duration attack detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
bssid	Basic service set ID	string	17
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
threatype	WIDS threat type	string	64
rsssi	The value of Received signal strength indicator	uint8	3
frametype	Frame Type	string	32
ds	Direction with distribution system	string	8
seq	Sequence	string	512
encrypt	The packet is encrypted or not	uint8	3
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
duration	Duration of the last threatening packed captured from TA	uint32	10

## 43535 - LOG\_ID\_EVENT\_WIRELESS\_WIDS\_WEP\_IV

**Message ID:** 43535

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WIDS\_WEP\_IV

**Message Meaning:** Wireless Weak WEP IV detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
bssid	Basic service set ID	string	17
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
threatype	WIDS threat type	string	64
rss	The value of Received signal strength indicator	uint8	3
frametype	Frame Type	string	32
ds	Direction with distribution system	string	8
seq	Sequence	string	512
encrypt	The packet is encrypted or not	uint8	3
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
weakwepiv	Weak Wep Initiation Vector	string	8

## 43542 - LOG\_ID\_EVENT\_WIRELESS\_WIDS\_EAPOL\_FLOOD

**Message ID:** 43542

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WIDS\_EAPOL\_FLOOD

**Message Meaning:** Wireless EAPOL packet flooding detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
manuf	Manufacturer name	string	20
live	Time in seconds	uint32	10
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
threattype	WIDS threat type	string	64
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
eapoltype	The packet type of EAPOL	string	16
eapolcnt	The count of EAPOL packets	uint32	10

**43544 - LOG\_ID\_EVENT\_WIRELESS\_WIDS\_MGMT\_FLOOD****Message ID:** 43544**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WIDS\_MGMT\_FLOOD**Message Meaning:** Wireless management flooding detected**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
bssid	Basic service set ID	string	17
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
threattype	WIDS threat type	string	64
rsi	The value of Received signal strength indicator	uint8	3
frametype	Frame Type	string	32
ds	Direction with distribution system	string	8
tamac	The MAC address of Transmitter. If none, then Receiver	string	17
mgmtcnt	The number of unauthorized client flooding managemet frames	uint32	10

## 43546 - LOG\_ID\_EVENT\_WIRELESS\_WIDS\_SPOOF\_DEAUTH

**Message ID:** 43546

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WIDS\_SPOOF\_DEAUTH

**Message Meaning:** Wireless spoofed deauthentication detected



**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
bssid	Basic service set ID	string	17
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
threattype	WIDS threat type	string	64
rss	The value of Received signal strength indicator	uint8	3
frametype	Frame Type	string	32
ds	Direction with distribution system	string	8
seq	Sequence	string	512
encrypt	The packet is encrypted or not	uint8	3
tamac	The MAC address of Transmitter. If none, then Receiver	string	17

## 43548 - LOG\_ID\_EVENT\_WIRELESS\_WIDS\_ASLEAP

**Message ID:** 43548

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WIDS\_ASLEAP

**Message Meaning:** Wireless Asleep attack detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
bssid	Basic service set ID	string	17
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
threatype	WIDS threat type	string	64
rss	The value of Received signal strength indicator	uint8	3
frametype	Frame Type	string	32

Log Field Name	Description	Data Type	Length
ds	Direction with distribution system	string	8
seq	Sequence	string	512
encrypt	The packet is encrypted or not	uint8	3
tamac	The MAC address of Transmitter. If none, then Receiver	string	17

## 43550 - LOG\_ID\_EVENT\_WIRELESS\_STA\_LOCATE

**Message ID:** 43550

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_LOCATE

**Message Meaning:** Wireless station presence detection

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
radioband	The operating radio band	string	64
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
stamac	The MAC address of wifi station	string	17

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
ap	Access Point	string	36
radioid	The operating radio ID	uint8	3

## 43551 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_JOIN

**Message ID:** 43551

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_JOIN

**Message Meaning:** Physical AP join

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19

Log Field Name	Description	Data Type	Length
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43552 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_LEAVE

**Message ID:** 43552

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_LEAVE

**Message Meaning:** Physical AP leave

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43553 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_FAIL

**Message ID:** 43553

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_FAIL

**Message Meaning:** Physical AP fail

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43554 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_UPDATE

**Message ID:** 43554

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_UPDATE

**Message Meaning:** Physical AP update

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43555 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_RESET

**Message ID:** 43555

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_RESET

**Message Meaning:** Physical AP reset

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43556 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_KICK

**Message ID:** 43556

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_KICK

**Message Meaning:** Physical AP kick

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10



Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43557 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_ADD\_FAILURE

**Message ID:** 43557

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_ADD\_FAILURE

**Message Meaning:** Physical AP add failure

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43558 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_CFG\_ERR

**Message ID:** 43558

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_CFG\_ERR

**Message Meaning:** Physical AP config error

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43559 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_SN\_MISMATCH

**Message ID:** 43559

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_SN\_MISMATCH

**Message Meaning:** Physical AP SN mismatch

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43560 - LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_RESTARTED

**Message ID:** 43560

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_RESTARTED

**Message Meaning:** Wireless system restarted

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 43561 - LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_HOSTAPD\_UP

**Message ID:** 43561

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_HOSTAPD\_UP

**Message Meaning:** Wireless system hostapd up

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 43562 - LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_HOSTAPD\_DOWN

**Message ID:** 43562

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_HOSTAPD\_DOWN

**Message Meaning:** Wireless system hostapd down

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 43563 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_DETECT

**Message ID:** 43563

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_DETECT

**Message Meaning:** Rogue AP detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36

Log Field Name	Description	Data Type	Length
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43564 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_OFFAIR

**Message ID:** 43564

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_OFFAIR

**Message Meaning:** Rogue AP off air

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3



Log Field Name	Description	Data Type	Length
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43565 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_ONAIR

**Message ID:** 43565

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_ONAIR

**Message Meaning:** Rogue AP on air

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36

Log Field Name	Description	Data Type	Length
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43566 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_OFFWIRE

**Message ID:** 43566

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_OFFWIRE

**Message Meaning:** Rogue AP off wire

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3

Log Field Name	Description	Data Type	Length
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43567 - LOG\_ID\_EVENT\_WIRELESS\_FAKEAP\_DETECT

**Message ID:** 43567

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_FAKEAP\_DETECT

**Message Meaning:** Fake AP detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36

Log Field Name	Description	Data Type	Length
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43568 - LOG\_ID\_EVENT\_WIRELESS\_FAKEAP\_ONAIR

**Message ID:** 43568

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_FAKEAP\_ONAIR

**Message Meaning:** Fake AP on air

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3

Log Field Name	Description	Data Type	Length
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43569 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_SUPPRESSED

**Message ID:** 43569

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_SUPPRESSED

**Message Meaning:** Rogue AP suppressed

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36



Log Field Name	Description	Data Type	Length
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43570 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_UNSUPPRESSED

**Message ID:** 43570

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_UNSUPPRESSED

**Message Meaning:** Rogue AP unsuppressed

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3

Log Field Name	Description	Data Type	Length
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43571 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_DETECT\_CHG

**Message ID:** 43571

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_DETECT\_CHG

**Message Meaning:** Rogue AP change detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36

Log Field Name	Description	Data Type	Length
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43572 - LOG\_ID\_EVENT\_WIRELESS\_STA ASSO

**Message ID:** 43572

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA ASSO

**Message Meaning:** Wireless client associated

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3

Log Field Name	Description	Data Type	Length
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43573 - LOG\_ID\_EVENT\_WIRELESS\_STA\_AUTH

**Message ID:** 43573

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_AUTH

**Message Meaning:** Wireless client authenticated

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43574 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DASS

**Message ID:** 43574

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DASS

**Message Meaning:** Wireless client disassociated

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43575 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DAUT

**Message ID:** 43575

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DAUT

**Message Meaning:** Wireless client deauthenticated

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256



Log Field Name	Description	Data Type	Length
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33
remotewtptime	The time of AP when client trying to connect	string	32

## 43576 - LOG\_ID\_EVENT\_WIRELESS\_STA\_IDLE

**Message ID:** 43576

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_IDLE

**Message Meaning:** Wireless client idle

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43577 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DENY

**Message ID:** 43577

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DENY

**Message Meaning:** Wireless client denied

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33
remotewtptime	The time of AP when client trying to connect	string	32

## 43578 - LOG\_ID\_EVENT\_WIRELESS\_STA\_KICK

**Message ID:** 43578

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_KICK

**Message Meaning:** Wireless client kicked

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64

Log Field Name	Description	Data Type	Length
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43579 - LOG\_ID\_EVENT\_WIRELESS\_STA\_IP

**Message ID:** 43579

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_IP

**Message Meaning:** Wireless client IP assigned

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12

Log Field Name	Description	Data Type	Length
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43580 - LOG\_ID\_EVENT\_WIRELESS\_STA\_LEAVE\_WTP

**Message ID:** 43580

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_LEAVE\_WTP

**Message Meaning:** Wireless client left WTP

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43581 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WTP\_DISCONN

**Message ID:** 43581

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WTP\_DISCONN

**Message Meaning:** Wireless client WTP disconnected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33



## 43582 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_CFG\_UNCLASSIFIED

**Message ID:** 43582

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_CFG\_UNCLASSIFIED

**Message Meaning:** Rogue AP status configured as unclassified

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43583 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_CFG\_ACCEPTED

**Message ID:** 43583

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_CFG\_ACCEPTED

**Message Meaning:** Rogue AP status configured as accepted

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43584 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_CFG\_ROGUE

**Message ID:** 43584**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_CFG\_ROGUE**Message Meaning:** Rogue AP status configured as rogue**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43585 - LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_CFG\_SUPPRESSED

**Message ID:** 43585

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ROGUE\_CFG\_SUPPRESSED

**Message Meaning:** Rogue AP status configured as suppressed

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43586 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DARRP\_CHAN

**Message ID:** 43586

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DARRP\_CHAN

**Message Meaning:** Physical AP radio DARRP channel change

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmode		string	10
operdrmmode		string	10

## 43587 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DARRP\_START

**Message ID:** 43587

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DARRP\_START

**Message Meaning:** Physical AP radio DARRP start

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmamode		string	10
operdrmmamode		string	10

## 43588 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_OPER\_CHAN

**Message ID:** 43588

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_OPER\_CHAN

**Message Meaning:** Physical AP radio operation channel change

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmode		string	10
operdrmmode		string	10

## 43589 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_RADAR

**Message ID:** 43589

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_RADAR

**Message Meaning:** Physical AP radio radar detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmamode		string	10
operdrmmamode		string	10

## 43590 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_NOL

**Message ID:** 43590

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_NOL

**Message Meaning:** Physical AP radio channel removed from NOL



**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmode		string	10
operdrmode		string	10

## 43591 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_COUNTRY\_CFG\_SUCCESS

**Message ID:** 43591

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_COUNTRY\_CFG\_SUCCESS

**Message Meaning:** Physical AP radio country config success

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10

Log Field Name	Description	Data Type	Length
opertxpower	The value of operating tx power	uint32	10
slctdrmmamode		string	10
operdrmmamode		string	10

## 43592 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_OPER\_COUNTRY

**Message ID:** 43592

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_OPER\_COUNTRY

**Message Meaning:** Physical AP radio operation country

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39

Log Field Name	Description	Data Type	Length
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmode		string	10
operdrmmode		string	10

## 43593 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_CFG\_TXPOWER

**Message ID:** 43593

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_CFG\_TXPOWER

**Message Meaning:** Physical AP radio config TX power

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmode		string	10
operdrmmode		string	10

## 43594 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_OPER\_TXPOWER

**Message ID:** 43594

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_OPER\_TXPOWER

**Message Meaning:** Physical AP radio operation TX power

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmamode		string	10
operdrmmamode		string	10

## 43595 - LOG\_ID\_EVENT\_WIRELESS\_CLB\_DENY

**Message ID:** 43595

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_CLB\_DENY

**Message Meaning:** Wireless client load balancing denied

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
stamac	The MAC address of wifi station	string	17
stacount	The count of wifi stations	uint32	10
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36

## 43596 - LOG\_ID\_EVENT\_WIRELESS\_CLB\_RETRY

**Message ID:** 43596

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_CLB\_RETRY

**Message Meaning:** Wireless client load balancing retry

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
stamac	The MAC address of wifi station	string	17
stacount	The count of wifi stations	uint32	10
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36

## 43597 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_ADD

**Message ID:** 43597

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_ADD

**Message Meaning:** Physical AP add

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10



Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43598 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_ADD\_XSS

**Message ID:** 43598

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_ADD\_XSS

**Message Meaning:** Physical AP add XSS

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43599 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_DEL

**Message ID:** 43599

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_DEL

**Message Meaning:** Physical AP delete

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43600 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DARRP\_STOP

**Message ID:** 43600

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DARRP\_STOP

**Message Meaning:** Physical AP radio DARRP stop

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrumode		string	10
operdrumode		string	10

## 43601 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_SIGNON

**Message ID:** 43601

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_SIGNON

**Message Meaning:** Wireless station sign on

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43602 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_SIGNON\_SUCCESS

**Message ID:** 43602

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_SIGNON\_SUCCESS

**Message Meaning:** Wireless station sign on success

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256

Log Field Name	Description	Data Type	Length
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43603 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_SIGNON\_FAILURE

**Message ID:** 43603

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_SIGNON\_FAILURE

**Message Meaning:** Wireless station sign on failed

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33

Log Field Name	Description	Data Type	Length
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43604 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_EMAIL\_REQUEST

**Message ID:** 43604

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_EMAIL\_REQUEST

**Message Meaning:** Captive-portal VAP e-mail collect request sent

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20



Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43605 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_EMAIL\_SUCCESS

**Message ID:** 43605

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_EMAIL\_SUCCESS

**Message Meaning:** Captive-portal VAP e-mail collect success

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43606 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_EMAIL\_FAILURE

**Message ID:** 43606

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_EMAIL\_FAILURE

**Message Meaning:** Captive-portal VAP e-mail collect failed

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256

Log Field Name	Description	Data Type	Length
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43607 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_DISCLAIMER\_CHECK

**Message ID:** 43607

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_DISCLAIMER\_CHECK

**Message Meaning:** Captive-portal VAP disclaimer agreed

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33

Log Field Name	Description	Data Type	Length
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43608 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_DISCLAIMER\_DECLINE

**Message ID:** 43608

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_DISCLAIMER\_DECLINE

**Message Meaning:** Captive-portal VAP disclaimer declined

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43609 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DARRP\_OPTIMIZATION\_START

**Message ID:** 43609

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DARRP\_OPTIMIZATION\_START

**Message Meaning:** DARRP optimization start

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmode		string	10
operdrmmode		string	10

**43610 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DARRP\_OPTIMIZATION\_STOP****Message ID:** 43610**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DARRP\_OPTIMIZATION\_STOP

**Message Meaning:** DARRP optimization stop

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmamode		string	10
operdrmamode		string	10



## 43611 - LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_UP

**Message ID:** 43611

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_UP

**Message Meaning:** Wireless controller start

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 43612 - LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_CFG\_LOADED

**Message ID:** 43612

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_CFG\_LOADED

**Message Meaning:** Wireless controller configuration loaded

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 43613 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_ERR

**Message ID:** 43613

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_ERR

**Message Meaning:** Physical AP error

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43614 - LOG\_ID\_EVENT\_WIRELESS\_DHCP\_STAVATION

**Message ID:** 43614

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_DHCP\_STAVATION

**Message Meaning:** DHCP Starvation detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
sn	Serial Number	string	64
ap	Access Point	string	36
vap	Virtual Access Point	string	36
source_mac	The source MAC address of wifi station	string	17
client_addr	Client address	string	17
xid		uint32	10
vapmode	Virtual Access Point mode	string	17

## 43615 - LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_IPSEC\_FAIL

**Message ID:** 43615

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_SYS\_AC\_IPSEC\_FAIL

**Message Meaning:** Wireless controller IPsec setup failed

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

## 43616 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_NOL\_ADD

**Message ID:** 43616

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_NOL\_ADD

**Message Meaning:** Physical AP radio NOL added

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39

Log Field Name	Description	Data Type	Length
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmode		string	10
operdrmmode		string	10

## 43618 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_IMAGE\_RC\_SUCCESS

**Message ID:** 43618

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_IMAGE\_RC\_SUCCESS

**Message Meaning:** Physical AP image receive success

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43619 - LOG\_ID\_EVENT\_WIRELESS\_OFFENDINGAP\_DETECT

**Message ID:** 43619

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_OFFENDINGAP\_DETECT

**Message Meaning:** Offending AP detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33

Log Field Name	Description	Data Type	Length
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43620 - LOG\_ID\_EVENT\_WIRELESS\_OFFENDINGAP\_ONAIR

**Message ID:** 43620

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_OFFENDINGAP\_ONAIR

**Message Meaning:** Offending AP on air

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning



Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
bssid	Basic service set ID	string	17
aptype	The AP type is Ad-hoc mode or regular AP mode	uint8	3
rate	WiFi band width rate	uint16	6
radioband	The operating radio band	string	64
channel	Channel	uint8	3
manuf	Manufacturer name	string	20
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
noise	WiFi signal noise level	int8	4
live	Time in seconds	uint32	10
age	Time in seconds - time passed since last seen	uint32	10
onwire	The rogue ap is onwire or not	string	3
detectionmethod	Detection Method	string	21
stamac	The MAC address of wifi station	string	17
apscan	The name of AP to detect rogue ap	string	36

Log Field Name	Description	Data Type	Length
sndetected	SN of the AP which detected the rogue AP	string	36
radioiddetected	The radio ID on the AP which detected the rogue ap	uint8	3
stacount	The count of wifi stations	uint32	10
snclosest	SN of the AP closest to the rogue AP	string	36
radioidclosest	The radio ID on the AP closest with the detected rogue ap	uint8	3
apstatus	Rogue AP status like unclassify(0), rogue(1), accept(2), suppress(3)	uint8	3

## 43621 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_DATA\_CHAN\_CHG

**Message ID:** 43621

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_DATA\_CHAN\_CHG

**Message Meaning:** Wireless wtp data channel changed

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36

Log Field Name	Description	Data Type	Length
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43622 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_VLAN\_PROBE

**Message ID:** 43622

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_VLAN\_PROBE

**Message Meaning:** WTP is probing vlan

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64

Log Field Name	Description	Data Type	Length
ip		ip	39
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43623 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_VLAN\_MISSING

**Message ID:** 43623

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_VLAN\_MISSING

**Message Meaning:** VLAN not detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39

Log Field Name	Description	Data Type	Length
meshmode	Mesh mode	string	19
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43624 - LOG\_ID\_EVENT\_WIRELESS\_WTP\_VLAN\_DETECTED

**Message ID:** 43624

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTP\_VLAN\_DETECTED

**Message Meaning:** VLAN detected

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
profile	Profile Name	string	64
ip		ip	39
meshmode	Mesh mode	string	19

Log Field Name	Description	Data Type	Length
snmeshparent	SN of the mesh parent	string	36
reason	Reason	string	256

## 43625 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_CMCC\_SUCCESS

**Message ID:** 43625

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_CMCC\_SUCCESS

**Message Meaning:** Wireless station CMCC sign on success

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4

Log Field Name	Description	Data Type	Length
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43626 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_CMCC\_FAILURE

**Message ID:** 43626

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_CMCC\_FAILURE

**Message Meaning:** Wireless station CMCC sign on failed

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43627 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_CMCC\_TIMEOUT

**Message ID:** 43627

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_CMCC\_TIMEOUT

**Message Meaning:** Wireless station CMCC sign on timeout

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10



Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43628 - LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_CMCC\_MAC\_AUTH\_SUCCESS

**Message ID:** 43628

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_CAP\_CMCC\_MAC\_AUTH\_SUCCESS

**Message Meaning:** Wireless station CMCC MAC auth success

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256

Log Field Name	Description	Data Type	Length
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
group	User group Name	string	64
srcip	Source IP	ip	39
snr		int8	4
mpsk	Multiple pre-shared keys	string	33

## 43629 - LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_AUTH\_FAILURE

**Message ID:** 43629

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_AUTH\_FAILURE

**Message Meaning:** Wireless client RADIUS authentication failure

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33

Log Field Name	Description	Data Type	Length
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43630 - LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_AUTH\_SUCCESS

**Message ID:** 43630

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_AUTH\_SUCCESS

**Message Meaning:** Wireless client RADIUS authentication success

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43631 - LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_AUTH\_NO\_RESP

**Message ID:** 43631

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_AUTH\_NO\_RESP

**Message Meaning:** Wireless client RADIUS authentication server not responding

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43632 - LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_MAC\_AUTH\_FAILURE

**Message ID:** 43632

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_MAC\_AUTH\_FAILURE

**Message Meaning:** Wireless client RADIUS MAC authentication failure

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43633 - LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_MAC\_AUTH\_SUCCESS

**Message ID:** 43633

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_MAC\_AUTH\_SUCCESS

**Message Meaning:** Wireless client RADIUS MAC authentication success

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43634 - LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_MAC\_AUTH\_NO\_RESP

**Message ID:** 43634

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_RADIUS\_MAC\_AUTH\_NO\_RESP

**Message Meaning:** Wireless client RADIUS MAC authentication server not responding

**Type:** Event

**Category:** WIRELESS



**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

**43635 - LOG\_ID\_EVENT\_WIRELESS\_STA\_OKC\_NO\_MATCH****Message ID:** 43635**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_OKC\_NO\_MATCH**Message Meaning:** Wireless client authenticates through OKC failed with no match

**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43636 - LOG\_ID\_EVENT\_WIRELESS\_STA\_OKC\_LOCAL\_MATCH

**Message ID:** 43636

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_OKC\_LOCAL\_MATCH**Message Meaning:** Wireless client authenticates through local OKC success**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43637 - LOG\_ID\_EVENT\_WIRELESS\_STA\_OKC\_INTER\_AC\_MATCH

**Message ID:** 43637

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_OKC\_INTER\_AC\_MATCH

**Message Meaning:** Wireless client authenticates through inter AC OKC success

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43638 - LOG\_ID\_EVENT\_WIRELESS\_STA\_OKC\_INTER\_AP\_MATCH

**Message ID:** 43638

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_OKC\_INTER\_AP\_MATCH

**Message Meaning:** Wireless client authenticates through inter AP OKC success

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43639 - LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_INVALID\_ACTION\_REQ

**Message ID:** 43639

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_INVALID\_ACTION\_REQ

**Message Meaning:** Wireless client sent invalid FT action request

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3

Log Field Name	Description	Data Type	Length
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43640 - LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_INVALID\_AUTH\_REQ

**Message ID:** 43640

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_INVALID\_AUTH\_REQ

**Message Meaning:** Wireless client sent invalid FT auth request

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43641 - LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_INVALID\_REASSOC\_REQ

**Message ID:** 43641

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_INVALID\_REASSOC\_REQ

**Message Meaning:** Wireless client sent invalid FT reassociation request

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16



Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43642 - LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_ACTION\_REQ

**Message ID:** 43642

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_ACTION\_REQ

**Message Meaning:** Wireless client sent FT action request

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43643 - LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_ACTION\_RESP

**Message ID:** 43643

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_ACTION\_RESP

**Message Meaning:** FT action response was sent to wireless client

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43644 - LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_AUTH\_REQ

**Message ID:** 43644

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_AUTH\_REQ

**Message Meaning:** Wireless client sent FT auth request

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

**43645 - LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_AUTH\_RESP****Message ID:** 43645**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_AUTH\_RESP**Message Meaning:** FT auth response was sent to wireless client

**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43646 - LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_REASSOC\_REQ

**Message ID:** 43646

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_REASSOC\_REQ**Message Meaning:** Wireless client sent FT reassociation request**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43647 - LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_REASSOC\_RESP

**Message ID:** 43647

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_FT\_REASSOC\_RESP

**Message Meaning:** FT reassociation response was sent to wireless client

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43648 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_INVALID\_SECOND\_MSG

**Message ID:** 43648

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_INVALID\_SECOND\_MSG

**Message Meaning:** Wireless client 4 way handshake failed with invalid 2/4 message

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64



Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43649 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_INVALID\_FOURTH\_MSG

**Message ID:** 43649

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_INVALID\_FOURTH\_MSG

**Message Meaning:** Wireless client 4 way handshake failed with invalid 4/4 message

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3

Log Field Name	Description	Data Type	Length
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43650 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_FIRST\_MSG

**Message ID:** 43650

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_FIRST\_MSG

**Message Meaning:** AP sent 1/4 message of 4 way handshake to wireless client

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43651 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_SECOND\_MSG

**Message ID:** 43651

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_SECOND\_MSG

**Message Meaning:** Wireless client sent 2/4 message of 4 way handshake

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43652 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_THIRD\_MSG

**Message ID:** 43652

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_THIRD\_MSG

**Message Meaning:** AP sent 3/4 message of 4 way handshake to wireless client

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43653 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_FOURTH\_MSG

**Message ID:** 43653

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_FOURTH\_MSG

**Message Meaning:** Wireless client sent 4/4 message of 4 way handshake

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43654 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_FIRST\_GROUP\_MSG

**Message ID:** 43654

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_FIRST\_GROUP\_MSG

**Message Meaning:** AP sent 1/2 message of group key handshake to wireless client

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

**43655 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_SECOND\_GROUP\_MSG****Message ID:** 43655**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_SECOND\_GROUP\_MSG**Message Meaning:** Wireless client sent 2/2 message of group key handshake

**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43656 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_MAX\_STA\_CNT

**Message ID:** 43656



**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_MAX\_STA\_CNT**Message Meaning:** Max sta count limit for the PSK was reached**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43657 - LOG\_ID\_EVENT\_WIRELESS\_STA\_ASSOC\_FAIL

**Message ID:** 43657

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_ASSOC\_FAIL

**Message Meaning:** Wireless station association failed

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43658 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_NO\_RESP

**Message ID:** 43658

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_NO\_RESP

**Message Meaning:** Wireless station DHCP process failed with no server response

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36

Log Field Name	Description	Data Type	Length
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43659 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_DIFF\_OFFER

**Message ID:** 43659

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_DIFF\_OFFER

**Message Meaning:** Another DHCP server sent DHCP offer to wireless station

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43660 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_NO\_ACK

**Message ID:** 43660

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_NO\_ACK

**Message Meaning:** No DHCP ACK from server

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43661 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_NAK

**Message ID:** 43661

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_NAK

**Message Meaning:** DHCP server sent DHCP NAK

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12

Log Field Name	Description	Data Type	Length
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43662 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_DUP\_IP

**Message ID:** 43662

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_DUP\_IP

**Message Meaning:** IP offered has been used by another wireless station

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40

Log Field Name	Description	Data Type	Length
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43663 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_DISCOVER

**Message ID:** 43663

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_DISCOVER

**Message Meaning:** Wireless station sent DHCP DISCOVER

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33



Log Field Name	Description	Data Type	Length
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43664 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_OFFER

**Message ID:** 43664

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_OFFER

**Message Meaning:** DHCP server sent DHCP OFFER

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43665 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_DECLINE

**Message ID:** 43665

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_DECLINE

**Message Meaning:** Wireless station sent DHCP DECLINE

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43666 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_REQUEST

**Message ID:** 43666

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_REQUEST

**Message Meaning:** Wireless station sent DHCP REQUEST

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43667 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_ACK

**Message ID:** 43667

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_ACK

**Message Meaning:** DHCP server sent DHCP ACK

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43668 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_RELEASE

**Message ID:** 43668

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_RELEASE

**Message Meaning:** Wireless station sent DHCP RELEASE

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43669 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_INFORM

**Message ID:** 43669

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_INFORM

**Message Meaning:** Wireless station sent DHCP INFORM

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43670 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_SELF\_ASSIGNED

**Message ID:** 43670

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP\_SELF\_ASSIGNED

**Message Meaning:** Wireless station is using self-assigned IP

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43671 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DNS\_NO\_RESP

**Message ID:** 43671

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DNS\_NO\_RESP

**Message Meaning:** Wireless station DNS process failed with no server response

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11



Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43672 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DNS\_SERVER\_FAILURE

**Message ID:** 43672

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DNS\_SERVER\_FAILURE

**Message Meaning:** Wireless station DNS process failed due to server failure

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43673 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DNS\_NO\_DOMAIN

**Message ID:** 43673

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DNS\_NO\_DOMAIN

**Message Meaning:** Wireless station DNS process failed due to non-existing domain

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43674 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_KRACK\_FT\_REASSOC

**Message ID:** 43674

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_KRACK\_FT\_REASSOC

**Message Meaning:** Wireless station WPA key reinstallation attack on FT reassociation

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43675 - LOG\_ID\_EVENT\_WIRELESS\_STA\_AUTH\_REQ

**Message ID:** 43675

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_AUTH\_REQ

**Message Meaning:** Authentication request from wireless station

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43676 - LOG\_ID\_EVENT\_WIRELESS\_STA\_AUTH\_RESP

**Message ID:** 43676

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_AUTH\_RESP

**Message Meaning:** Authentication response to wireless station

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

**43677 - LOG\_ID\_EVENT\_WIRELESS\_STA\_ASSOC\_REQ****Message ID:** 43677**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_ASSOC\_REQ**Message Meaning:** Association request from wireless station

**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43678 - LOG\_ID\_EVENT\_WIRELESS\_STA\_REASSOC\_REQ

**Message ID:** 43678

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_REASSOC\_REQ**Message Meaning:** Reassociation request from wireless station**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32



## 43679 - LOG\_ID\_EVENT\_WIRELESS\_STA\_ASSOC\_RESP

**Message ID:** 43679

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_ASSOC\_RESP

**Message Meaning:** Association response to wireless station

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3

Log Field Name	Description	Data Type	Length
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43680 - LOG\_ID\_EVENT\_WIRELESS\_STA\_REASSOC\_RESP

**Message ID:** 43680

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_REASSOC\_RESP

**Message Meaning:** Reassociation response to wireless station

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43681 - LOG\_ID\_EVENT\_WIRELESS\_STA\_PROBE\_REQ

**Message ID:** 43681

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_PROBE\_REQ

**Message Meaning:** Probe request from wireless station

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3

Log Field Name	Description	Data Type	Length
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43682 - LOG\_ID\_EVENT\_WIRELESS\_STA\_PROBE\_RESP

**Message ID:** 43682

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_PROBE\_RESP

**Message Meaning:** Probe response to wireless station

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43683 - LOG\_ID\_EVENT\_WIRELESS\_BLE\_DEV\_LOCATE

**Message ID:** 43683

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_BLE\_DEV\_LOCATE

**Message Meaning:** Wireless ble dev detection

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36

## 43684 - LOG\_ID\_EVENT\_WIRELESS\_ADDRGRP\_DUPLICATE\_MAC

**Message ID:** 43684

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ADDRGRP\_DUPLICATE\_MAC

**Message Meaning:** Wireless addrgrp duplicate mac

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
action	Policy Action	string	65
msg	Log Message	string	4096
addrgrp		string	36

## 43685 - LOG\_ID\_EVENT\_WIRELESS\_ADDRGRP\_ADDR\_APPLY

**Message ID:** 43685

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_ADDRGRP\_ADDR\_APPLY

**Message Meaning:** Wireless addrgrp address apply

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
addrgrp		string	36

## 43686 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_INVALID\_SCHEDULE

**Message ID:** 43686

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WPA\_MSG\_INVALID\_SCHEDULE

**Message Meaning:** PSK is out of any valid schedules

**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43687 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WL\_BRIDGE\_TRAFFIC\_STATS

**Message ID:** 43687



**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WL\_BRIDGE\_TRAFFIC\_STATS

**Message Meaning:** Traffic stats for station with bridge wlan

**Type:** Event

**Category:** WIRELESS

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
signal	The signal value of SSID or client	int8	4
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
vap	Virtual Access Point	string	36
user	User name of authenticated user	string	256
srcip	Source IP	ip	39
snr		int8	4
sentbyte	Bytes Sent	uint64	20
rcvdbyte	Received Bytes	uint64	20
nextstat	Time interval in seconds for the next statistics	uint32	10

## 43688 - LOG\_ID\_EVENT\_WIRELESS\_APCFG\_RECEIVE

**Message ID:** 43688

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_APCFG\_RECEIVE

**Message Meaning:** FortiAP receives the apcfg

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256

## 43689 - LOG\_ID\_EVENT\_WIRELESS\_APCFG\_VALIDATING

**Message ID:** 43689

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_APCFG\_VALIDATING

**Message Meaning:** FortiAP is validating the apcfg

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256

## 43690 - LOG\_ID\_EVENT\_WIRELESS\_APCFG\_APPLY

**Message ID:** 43690

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_APCFG\_APPLY

**Message Meaning:** FortiAP applies the apcfg

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256

## 43691 - LOG\_ID\_EVENT\_WIRELESS\_APCFG\_REJECT

**Message ID:** 43691

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_APCFG\_REJECT

**Message Meaning:** FortiAP rejects the apcfg

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256

## 43692 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_ANTENNA\_DEFECT\_DETECT

**Message ID:** 43692

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_ANTENNA\_DEFECT\_DETECT

**Message Meaning:** Defect antenna detection

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64

Log Field Name	Description	Data Type	Length
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmode		string	10
operdrmmode		string	10

## 43693 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WNM\_ACTION\_BSTM\_REQ

**Message ID:** 43693

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WNM\_ACTION\_BSTM\_REQ

**Message Meaning:** AP sent WNM action BSTM request

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43694 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WNM\_ACTION\_BSTM\_RESP\_ACCEPT

**Message ID:** 43694

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WNM\_ACTION\_BSTM\_RESP\_ACCEPT

**Message Meaning:** Wireless client sent WNM action BSTM response accept

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43695 - LOG\_ID\_EVENT\_WIRELESS\_STA\_WNM\_ACTION\_BSTM\_RESP\_REJECT

**Message ID:** 43695

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_WNM\_ACTION\_BSTM\_RESP\_REJECT

**Message Meaning:** Wireless client sent WNM action BSTM response reject

**Type:** Event

**Category:** WIRELESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8



Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
channel	Channel	uint8	3
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64
ap	Access Point	string	36
reason	Reason	string	256
vap	Virtual Access Point	string	36
radioid	The operating radio ID	uint8	3
user	User name of authenticated user	string	256
remotewtptime	The time of AP when client trying to connect	string	32

## 43696 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DRMA\_START

**Message ID:** 43696

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DRMA\_START

**Message Meaning:** Physical AP radio DRMA start

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmamode		string	10
operdrmamode		string	10

## 43697 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DRMA\_STOP

**Message ID:** 43697

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DRMA\_STOP

**Message Meaning:** Physical AP radio DRMA stop

**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrumode		string	10
operdrumode		string	10

**43698 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DRMA\_MODE****Message ID:** 43698**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_DRMA\_MODE**Message Meaning:** Physical AP radio DRMA mode**Type:** Event**Category:** WIRELESS**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10

Log Field Name	Description	Data Type	Length
opertxpower	The value of operating tx power	uint32	10
slctdrmmamode		string	10
operdrmmamode		string	10

## 43699 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_SOLICIT

**Message ID:** 43699

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_SOLICIT

**Message Meaning:** Wireless station sent DHCP6 SOLICIT

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43700 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_ADVERTISE

**Message ID:** 43700

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_ADVERTISE

**Message Meaning:** DHCP6 server sent DHCP6 ADVERTISE

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43701 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_REQUEST

**Message ID:** 43701

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_REQUEST

**Message Meaning:** Wireless station sent DHCP6 REQUEST

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43702 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_CONFIRM

**Message ID:** 43702

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_CONFIRM

**Message Meaning:** Wireless station sent DHCP6 CONFIRM

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64



Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43703 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_RENEW

**Message ID:** 43703

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_RENEW

**Message Meaning:** Wireless station sent DHCP6 RENEW

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43704 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_REPLY

**Message ID:** 43704

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_REPLY

**Message Meaning:** DHCP6 server sent DHCP6 REPLY

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43705 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_RELEASE

**Message ID:** 43705

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_RELEASE

**Message Meaning:** Wireless station sent DHCP6 RELEASE

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43706 - LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_RECONFIGURE

**Message ID:** 43706

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_STA\_DHCP6\_RECONFIGURE

**Message Meaning:** DHCP6 server sent DHCP6 RECONFIGURE

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
security	Security	string	40
encryption	The encryption type of detected rogue AP	string	12
stamac	The MAC address of wifi station	string	17
sn	Serial Number	string	64

Log Field Name	Description	Data Type	Length
ap	Access Point	string	36
vap	Virtual Access Point	string	36
remotewtptime	The time of AP when client trying to connect	string	32

## 43707 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_SSID\_UP

**Message ID:** 43707

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_SSID\_UP

**Message Meaning:** Physical AP radio ssid up

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39

Log Field Name	Description	Data Type	Length
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmode		string	10
operdrmmode		string	10

## 43708 - LOG\_ID\_EVENT\_WIRELESS\_WTPR\_SSID\_DOWN

**Message ID:** 43708

**Message Description:** LOG\_ID\_EVENT\_WIRELESS\_WTPR\_SSID\_DOWN

**Message Meaning:** Physical AP radio ssid down

**Type:** Event

**Category:** WIRELESS

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
ssid	WiFi Service Set ID	string	33
radioband	The operating radio band	string	64
sn	Serial Number	string	64
ap	Access Point	string	36
ip		ip	39
radioid	The operating radio ID	uint8	3
bandwidth	Bandwidth	string	42
configcountry	Config Country	string	4
opercountry	The name of operating country on a AP	string	4
cfgtxpower	Config TX power	uint32	10
opertxpower	The value of operating tx power	uint32	10
slctdrmmode		string	10
operdrmmode		string	10

## 43776 - LOG\_ID\_EVENT\_NAC\_QUARANTINE

**Message ID:** 43776

**Message Description:** LOG\_ID\_EVENT\_NAC\_QUARANTINE

**Message Meaning:** NAC quarantine

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096
service	Name of Service	string	64
proto	Protocol Number	uint8	3
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
duration	Duration	uint32	10
src_int	Source Interface	string	64
dst_int	Destination Interface	string	64
banned_src	NAC quarantine Banned Source IP	string	16
admin	Administrator	string	64
group	User group Name	string	64
policyid	Policy ID	uint32	10
banned_rule	NAC quarantine Banned Rule Name	string	80
sensor	NAC Sensor Name	string	36

## 43777 - LOG\_ID\_EVENT\_NAC\_ANOMALY\_QUARANTINE

**Message ID:** 43777

**Message Description:** LOG\_ID\_EVENT\_NAC\_ANOMALY\_QUARANTINE

**Message Meaning:** NAC anomaly quarantine

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice



Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096
service	Name of Service	string	64
proto	Protocol Number	uint8	3
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
duration	Duration	uint32	10
src_int	Source Interface	string	64
dst_int	Destination Interface	string	64
banned_src	NAC quarantine Banned Source IP	string	16
admin	Administrator	string	64
group	User group Name	string	64
policyid	Policy ID	uint32	10
banned_rule	NAC quarantine Banned Rule Name	string	80
sensor	NAC Sensor Name	string	36

## 43800 - LOG\_ID\_EVENT\_ELBC\_BLADE\_JOIN

**Message ID:** 43800

**Message Description:** LOG\_ID\_EVENT\_ELBC\_BLADE\_JOIN

**Message Meaning:** Blade ready to process traffic

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
informationsource	Information Source	string	4096
slot	Slot Number	uint8	3
chassisid	Chassis ID	uint8	3

## 43801 - LOG\_ID\_EVENT\_ELBC\_BLADE\_LEAVE

**Message ID:** 43801

**Message Description:** LOG\_ID\_EVENT\_ELBC\_BLADE\_LEAVE

**Message Meaning:** Blade not ready to process traffic

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
informationsource	Information Source	string	4096
slot	Slot Number	uint8	3
chassisid	Chassis ID	uint8	3

## 43802 - LOG\_ID\_EVENT\_ELBC\_MASTER\_BLADE\_FOUND

**Message ID:** 43802

**Message Description:** LOG\_ID\_EVENT\_ELBC\_MASTER\_BLADE\_FOUND

**Message Meaning:** Primary blade found

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
informationsource	Information Source	string	4096
slot	Slot Number	uint8	3
chassisid	Chassis ID	uint8	3

## 43803 - LOG\_ID\_EVENT\_ELBC\_MASTER\_BLADE\_LOST

**Message ID:** 43803

**Message Description:** LOG\_ID\_EVENT\_ELBC\_MASTER\_BLADE\_LOST

**Message Meaning:** Primary blade lost

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
informationsource	Information Source	string	4096
slot	Slot Number	uint8	3
chassisid	Chassis ID	uint8	3

## 43804 - LOG\_ID\_EVENT\_ELBC\_MASTER\_BLADE\_CHANGE

**Message ID:** 43804

**Message Description:** LOG\_ID\_EVENT\_ELBC\_MASTER\_BLADE\_CHANGE

**Message Meaning:** Primary blade changed

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
informationsource	Information Source	string	4096
oldslot	Original Slot Number	uint8	3

Log Field Name	Description	Data Type	Length
oldchassisid	Original Chassis Number	uint8	3
newslot	New Slot Number	uint8	3
newchassisid	New Chassis ID	uint8	3

## 43805 - LOG\_ID\_EVENT\_ELBC\_ACTIVE\_CHANNEL\_FOUND

**Message ID:** 43805

**Message Description:** LOG\_ID\_EVENT\_ELBC\_ACTIVE\_CHANNEL\_FOUND

**Message Meaning:** ELBC channel active

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
informationsource	Information Source	string	4096
slot	Slot Number	uint8	3
chassisid	Chassis ID	uint8	3
newchannel	New Channel Number	uint8	3

## 43806 - LOG\_ID\_EVENT\_ELBC\_ACTIVE\_CHANNEL\_LOST

**Message ID:** 43806

**Message Description:** LOG\_ID\_EVENT\_ELBC\_ACTIVE\_CHANNEL\_LOST

**Message Meaning:** ELBC channel inactive

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
informationsource	Information Source	string	4096
slot	Slot Number	uint8	3
chassisid	Chassis ID	uint8	3
oldchannel	Original Channel Number	uint8	3

## 43807 - LOG\_ID\_EVENT\_ELBC\_ACTIVE\_CHANNEL\_CHANGE

**Message ID:** 43807

**Message Description:** LOG\_ID\_EVENT\_ELBC\_ACTIVE\_CHANNEL\_CHANGE

**Message Meaning:** ELBC channel failover

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
informationsource	Information Source	string	4096
slot	Slot Number	uint8	3
chassisid	Chassis ID	uint8	3
newchannel	New Channel Number	uint8	3
oldchannel	Original Channel Number	uint8	3

## 43808 - LOG\_ID\_EVENT\_ELBC\_CHASSIS\_ACTIVE

**Message ID:** 43808**Message Description:** LOG\_ID\_EVENT\_ELBC\_CHASSIS\_ACTIVE**Message Meaning:** ELBC chassis active**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8



Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
informationsource	Information Source	string	4096
chassisid	Chassis ID	uint8	3

## 43809 - LOG\_ID\_EVENT\_ELBC\_CHASSIS\_INACTIVE

**Message ID:** 43809

**Message Description:** LOG\_ID\_EVENT\_ELBC\_CHASSIS\_INACTIVE

**Message Meaning:** ELBC chassis inactive

**Type:** Event

**Category:** SYSTEM

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
msg	Log Message	string	4096
informationsource	Information Source	string	4096
chassisid	Chassis ID	uint8	3

## 44544 - LOGID\_EVENT\_CONFIG\_PATH

**Message ID:** 44544

**Message Description:** LOGID\_EVENT\_CONFIG\_PATH

**Message Meaning:** Path configured

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
cfgtid	Config transaction id	uint32	10
cfgpath	Configuration path	string	128

## 44545 - LOGID\_EVENT\_CONFIG\_OBJ

**Message ID:** 44545

**Message Description:** LOGID\_EVENT\_CONFIG\_OBJ

**Message Meaning:** Object configured

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
cfgtid	Config transaction id	uint32	10
cfgpath	Configuration path	string	128
cfgobj	Configuration object	string	256

## 44546 - LOGID\_EVENT\_CONFIG\_ATTR

**Message ID:** 44546

**Message Description:** LOGID\_EVENT\_CONFIG\_ATTR

**Message Meaning:** Attribute configured

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
cfgtid	Config transaction id	uint32	10
cfgpath	Configuration path	string	128
cfgattr	Configuration attribute	string	4096

## 44547 - LOGID\_EVENT\_CONFIG\_OBJATTR

**Message ID:** 44547

**Message Description:** LOGID\_EVENT\_CONFIG\_OBJATTR

**Message Meaning:** Object attribute configured

**Type:** Event

**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
cfgtid	Config transaction id	uint32	10
cfgpath	Configuration path	string	128
cfgobj	Configuration object	string	256
cfgattr	Configuration attribute	string	4096

## 44548 - LOGID\_EVENT\_CONFIG\_EXEC

**Message ID:** 44548**Message Description:** LOGID\_EVENT\_CONFIG\_EXEC**Message Meaning:** Action performed**Type:** Event**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

## 44549 - LOGID\_EVENT\_CONFIG\_OBJATTR\_MTNER

**Message ID:** 44549

**Message Description:** LOGID\_EVENT\_CONFIG\_OBJATTR\_MTNER

**Message Meaning:** Object attribute configured by maintainer

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
cfgtid	Config transaction id	uint32	10
cfgpath	Configuration path	string	128
cfgobj	Configuration object	string	256
cfgattr	Configuration attribute	string	4096

## 44550 - LOGID\_EVENT\_CONFIG\_OBJ\_MTNER

**Message ID:** 44550

**Message Description:** LOGID\_EVENT\_CONFIG\_OBJ\_MTNER

**Message Meaning:** Object configured by maintainer

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
cfgtid	Config transaction id	uint32	10
cfgpath	Configuration path	string	128
cfgobj	Configuration object	string	256

## 44551 - LOGID\_EVENT\_CONFIG\_ATTR\_MTNER

**Message ID:** 44551

**Message Description:** LOGID\_EVENT\_CONFIG\_ATTR\_MTNER

**Message Meaning:** Attribute configured by maintainer

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256



Log Field Name	Description	Data Type	Length
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096
cfgtid	Config transaction id	uint32	10
cfgpath	Configuration path	string	128
cfgattr	Configuration attribute	string	4096

## 44552 - LOGID\_EVENT\_CONFIG\_PATH\_MTNER

**Message ID:** 44552

**Message Description:** LOGID\_EVENT\_CONFIG\_PATH\_MTNER

**Message Meaning:** Path configured by maintainer

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ui	User Interface	string	64
action	Policy Action	string	65
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
cfgtid	Config transaction id	uint32	10
cfgpath	Configuration path	string	128

## 44553 - LOGID\_EVENT\_CONFIG\_FIXEDPORT\_DIS

**Message ID:** 44553

**Message Description:** LOGID\_EVENT\_CONFIG\_FIXEDPORT\_DIS

**Message Meaning:** Policy attribute fixed port changed during upgrade

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
policyid	Policy ID	uint32	10

## 44554 - LOGID\_EVENT\_CONFIG\_POL\_CHANGED

**Message ID:** 44554

**Message Description:** LOGID\_EVENT\_CONFIG\_POL\_CHANGED

**Message Meaning:** Learning mode policy is converted to accept policy during upgrade.

**Type:** Event

**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
policyid	Policy ID	uint32	10

## 44555 - LOGID\_EVENT\_CMDB\_DEADLOCK\_DETECTED

**Message ID:** 44555**Message Description:** LOGID\_EVENT\_CMDB\_DEADLOCK\_DETECTED**Message Meaning:** CMDB lock deadlock is detected.**Type:** Event**Category:** SYSTEM**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 45057 - LOG\_ID\_FCC\_ADD

**Message ID:** 45057

**Message Description:** LOG\_ID\_FCC\_ADD

**Message Meaning:** FortiClient connection added

**Type:** Event

**Category:** ENDPOINT

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
license_limit	Maximum Number of FortiClients for the License	string	32
used_for_type	Connection for the type	uint32	10

Log Field Name	Description	Data Type	Length
connection_type	FortiClient Connection Type	string	6
count	Count of EndPoint Connections	uint32	10
user	User name of authenticated user	string	256
ip	Source IP	ip	39
name	Display Name of the Connection	string	128
fctuid	FortiClient UID	string	32
msg	Log Message	string	4096

## 45058 - LOG\_ID\_FCC\_CLOSE

**Message ID:** 45058

**Message Description:** LOG\_ID\_FCC\_CLOSE

**Message Meaning:** FortiClient connection closed

**Type:** Event

**Category:** ENDPOINT

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 45061 - LOG\_ID\_FCC\_CLOSE\_BY\_TYPE

**Message ID:** 45061

**Message Description:** LOG\_ID\_FCC\_CLOSE\_BY\_TYPE

**Message Meaning:** FortiClient connection closed by type

**Type:** Event

**Category:** ENDPOINT

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
license_limit	Maximum Number of FortiClients for the License	string	32
used_for_type	Connection for the type	uint32	10
connection_type	FortiClient Connection Type	string	6
count	Count of EndPoint Connections	uint32	10
user	User name of authenticated user	string	256
ip	Source IP	ip	39
name	Display Name of the Connection	string	128
fctuid	FortiClient UID	string	32
msg	Log Message	string	4096

## 45071 - LOG\_ID\_FCC\_VULN\_SCAN

**Message ID:** 45071

**Message Description:** LOG\_ID\_FCC\_VULN\_SCAN

**Message Meaning:** FortiClient Vulnerability Scan

**Type:** Event

**Category:** ENDPOINT**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
fctuid	FortiClient UID	string	32
msg	Log Message	string	4096
scantime		uint64	20
srcip	Source IP	ip	39
srcname	Source name	string	64
srcmac	Source MAC address	string	17
vulnid	Vulnerability ID	uint32	10
vulnname	Vulnerability name	string	128
vulncat	Vulnerability Category	string	32
severity	Severity	string	10
cveid	CVE ID	string	720
vendorurl		string	256
devtype	Device type	string	32

## 45114 - LOG\_ID\_EC\_REG\_QUARANTINE

**Message ID:** 45114**Message Description:** LOG\_ID\_EC\_REG\_QUARANTINE

**Message Meaning:** FortiClient endpoint quarantined

**Type:** Event

**Category:** ENDPOINT

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ip	Source IP	ip	39
fctuid	FortiClient UID	string	32
msg	Log Message	string	4096
fctemssn		string	16
hostname	Hostname	string	128

## 45115 - LOG\_ID\_EC\_REG\_UNQUARANTINE

**Message ID:** 45115

**Message Description:** LOG\_ID\_EC\_REG\_UNQUARANTINE

**Message Meaning:** FortiClient endpoint quarantine removed

**Type:** Event

**Category:** ENDPOINT

**Severity:** Notice



Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
ip	Source IP	ip	39
fctuid	FortiClient UID	string	32
msg	Log Message	string	4096
fctemssn		string	16
hostname	Hostname	string	128

## 46000 - LOG\_ID\_VIP\_REAL\_SVR\_ENA

**Message ID:** 46000

**Message Description:** LOG\_ID\_VIP\_REAL\_SVR\_ENA

**Message Meaning:** VIP real server enabled

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
server	Server IP Address	string	64
port	Port Number	uint16	5
vip	Virtual IP	string	64

## 46001 - LOG\_ID\_VIP\_REAL\_SVR\_DISA

**Message ID:** 46001

**Message Description:** LOG\_ID\_VIP\_REAL\_SVR\_DISA

**Message Meaning:** VIP real server disabled

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32

Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
server	Server IP Address	string	64
port	Port Number	uint16	5
vip	Virtual IP	string	64

## 46002 - LOG\_ID\_VIP\_REAL\_SVR\_UP

**Message ID:** 46002

**Message Description:** LOG\_ID\_VIP\_REAL\_SVR\_UP

**Message Meaning:** VIP real server up

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65

Log Field Name	Description	Data Type	Length
status	Status	string	23
msg	Log Message	string	4096
server	Server IP Address	string	64
port	Port Number	uint16	5
vip	Virtual IP	string	64

## 46003 - LOG\_ID\_VIP\_REAL\_SVR\_DOWN

**Message ID:** 46003

**Message Description:** LOG\_ID\_VIP\_REAL\_SVR\_DOWN

**Message Meaning:** VIP real server down

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
server	Server IP Address	string	64
port	Port Number	uint16	5
vip	Virtual IP	string	64

## 46004 - LOG\_ID\_VIP\_REAL\_SVR\_ENT\_HOLDDOWN

**Message ID:** 46004

**Message Description:** LOG\_ID\_VIP\_REAL\_SVR\_ENT\_HOLDDOWN

**Message Meaning:** VIP real server entered hold-down

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
server	Server IP Address	string	64
port	Port Number	uint16	5
vip	Virtual IP	string	64

## 46005 - LOG\_ID\_VIP\_REAL\_SVR\_FAIL\_HOLDDOWN

**Message ID:** 46005

**Message Description:** LOG\_ID\_VIP\_REAL\_SVR\_FAIL\_HOLDDOWN

**Message Meaning:** VIP real server health check failed during hold-down

**Type:** Event

**Category:** SYSTEM

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
server	Server IP Address	string	64
port	Port Number	uint16	5
vip	Virtual IP	string	64

## 46006 - LOG\_ID\_VIP\_REAL\_SVR\_FAIL

**Message ID:** 46006**Message Description:** LOG\_ID\_VIP\_REAL\_SVR\_FAIL**Message Meaning:** VIP real server health check failed**Type:** Event**Category:** SYSTEM**Severity:** Debug

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
action	Policy Action	string	65
status	Status	string	23
msg	Log Message	string	4096
server	Server IP Address	string	64
port	Port Number	uint16	5
vip	Virtual IP	string	64
monitor-name	Health Monitor Type	string	35
monitor-type	Health Monitor Name	string	32

## 46400 - LOG\_ID\_EVENT\_EXT\_SYS

**Message ID:** 46400

**Message Description:** LOG\_ID\_EVENT\_EXT\_SYS

**Message Meaning:** FortiExtender system activity

**Type:** Event

**Category:** FORTIEXTENDER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46401 - LOG\_ID\_EVENT\_EXT\_LOCAL

**Message ID:** 46401

**Message Description:** LOG\_ID\_EVENT\_EXT\_LOCAL

**Message Meaning:** FortiExtender controller activity

**Type:** Event

**Category:** FORTIEXTENDER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 46402 - LOG\_ID\_EVENT\_EXT\_LOCAL\_ERROR

**Message ID:** 46402

**Message Description:** LOG\_ID\_EVENT\_EXT\_LOCAL\_ERROR



**Message Meaning:** FortiExtender controller activity error

**Type:** Event

**Category:** FORTIEXTENDER

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 46403 - LOG\_ID\_EVENT\_EXT\_REMOTE\_EMERG

**Message ID:** 46403

**Message Description:** LOG\_ID\_EVENT\_EXT\_REMOTE\_EMERG

**Message Meaning:** Remote FortiExtender emergency activity

**Type:** Event

**Category:** FORTIEXTENDER

**Severity:** Emergency

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
ip		ip	39

## 46404 - LOG\_ID\_EVENT\_EXT\_REMOTE\_ALERT

**Message ID:** 46404

**Message Description:** LOG\_ID\_EVENT\_EXT\_REMOTE\_ALERT

**Message Meaning:** Remote FortiExtender alert activity

**Type:** Event

**Category:** FORTIEXTENDER

**Severity:** Alert

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
ip		ip	39

## 46405 - LOG\_ID\_EVENT\_EXT\_REMOTE\_CRITICAL

**Message ID:** 46405

**Message Description:** LOG\_ID\_EVENT\_EXT\_REMOTE\_CRITICAL

**Message Meaning:** Remote FortiExtender critical activity

**Type:** Event

**Category:** FORTIEXTENDER

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
ip		ip	39

## 46406 - LOG\_ID\_EVENT\_EXT\_REMOTE\_ERROR

**Message ID:** 46406

**Message Description:** LOG\_ID\_EVENT\_EXT\_REMOTE\_ERROR

**Message Meaning:** Remote FortiExtender error activity

**Type:** Event

**Category:** FORTIEXTENDER

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
ip		ip	39

## 46407 - LOG\_ID\_EVENT\_EXT\_REMOTE\_WARNING

**Message ID:** 46407

**Message Description:** LOG\_ID\_EVENT\_EXT\_REMOTE\_WARNING

**Message Meaning:** Remote FortiExtender warning activity

**Type:** Event

**Category:** FORTIEXTENDER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
ip		ip	39

## 46408 - LOG\_ID\_EVENT\_EXT\_REMOTE\_NOTIF

**Message ID:** 46408

**Message Description:** LOG\_ID\_EVENT\_EXT\_REMOTE\_NOTIF

**Message Meaning:** Remote FortiExtender notify activity

**Type:** Event

**Category:** FORTIEXTENDER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
ip		ip	39

## 46409 - LOG\_ID\_EVENT\_EXT\_REMOTE\_INFO

**Message ID:** 46409

**Message Description:** LOG\_ID\_EVENT\_EXT\_REMOTE\_INFO

**Message Meaning:** Remote FortiExtender info activity

**Type:** Event

**Category:** FORTIEXTENDER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
ip		ip	39

## 46410 - LOG\_ID\_EVENT\_EXT\_REMOTE\_DEBUG

**Message ID:** 46410

**Message Description:** LOG\_ID\_EVENT\_EXT\_REMOTE\_DEBUG

**Message Meaning:** Remote FortiExtender debug activity

**Type:** Event

**Category:** FORTIEXTENDER

**Severity:** Debug

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
sn	Serial Number	string	64
ip		ip	39

## 46501 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_DETECTION

**Message ID:** 46501

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_DETECTION

**Message Meaning:** LTE modem detection

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46502 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_GPSD

**Message ID:** 46502

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_GPSD

**Message Meaning:** LTE modem GPS daemon started or stopped

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46503 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_GPS\_LOC\_ACQUISITION

**Message ID:** 46503

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_GPS\_LOC\_ACQUISITION

**Message Meaning:** LTE modem GPS location acquisition



**Type:** Event**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46504 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_BILLD

**Message ID:** 46504**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_BILLD**Message Meaning:** LTE modem billing daemon started or stopped**Type:** Event**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46505 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_BILLING\_PURGED

**Message ID:** 46505

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_BILLING\_PURGED

**Message Meaning:** LTE billing data purged

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46506 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_BILLING\_DAILY\_LOG

**Message ID:** 46506

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_BILLING\_DAILY\_LOG

**Message Meaning:** LTE billing daily usage information

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46507 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_FW\_UPGRADE

**Message ID:** 46507

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_FW\_UPGRADE

**Message Meaning:** LTE modem firmware upgrade event

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46508 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_QDL\_DETECTION

**Message ID:** 46508

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_QDL\_DETECTION

**Message Meaning:** LTE modem QDL device detection event

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46509 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_REBOOT

**Message ID:** 46509

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_REBOOT**Message Meaning:** LTE modem reboot event**Type:** Event**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46510 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_OP\_MODE

**Message ID:** 46510**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_OP\_MODE**Message Meaning:** LTE modem operation mode**Type:** Event**Category:** SYSTEM**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46511 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_POWER\_ON\_OFF

**Message ID:** 46511

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_POWER\_ON\_OFF

**Message Meaning:** LTE modem powered on or powered off

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46512 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_SIM\_STATE

**Message ID:** 46512

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_SIM\_STATE

**Message Meaning:** LTE modem sim card state event

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46513 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_LINK\_CONNECTION

**Message ID:** 46513

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_LINK\_CONNECTION

**Message Meaning:** LTE modem data link connection event

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46514 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_MANUAL\_HANOVER

**Message ID:** 46514

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_MANUAL\_HANOVER

**Message Meaning:** LTE modem manual handover event

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096



## 46515 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_IP\_ADDR

**Message ID:** 46515

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_IP\_ADDR

**Message Meaning:** LTE modem ip address event

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46516 - LOG\_ID\_INTERNAL\_LTE\_MODEM\_BEARER\_TECH\_CHANGE

**Message ID:** 46516

**Message Description:** LOG\_ID\_INTERNAL\_LTE\_MODEM\_BEARER\_TECH\_CHANGE

**Message Meaning:** LTE modem bearer event

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 46600 - LOG\_ID\_EVENT\_AUTOMATION\_TRIGGERED

**Message ID:** 46600

**Message Description:** LOG\_ID\_EVENT\_AUTOMATION\_TRIGGERED

**Message Meaning:** Automation stitch triggered

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
stitch	Automation stitch name	string	36
trigger	Automation trigger name	string	36
stitchaction		string	256
from	Sender Email Address for Notification	string	128

## 46900 - LOG\_ID\_POE\_STATUS\_REPORT

**Message ID:** 46900

**Message Description:** LOG\_ID\_POE\_STATUS\_REPORT

**Message Meaning:** PoE device status reported

**Type:** Event

**Category:** SYSTEM

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 47000 - LOG\_ID\_MALWARE\_LIST\_TRUNCATED\_ENTER

**Message ID:** 47000

**Message Description:** LOG\_ID\_MALWARE\_LIST\_TRUNCATED\_ENTER

**Message Meaning:** External malware list is truncated

**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 47001 - LOG\_ID\_MALWARE\_LIST\_TRUNCATED\_EXIT

**Message ID:** 47001**Message Description:** LOG\_ID\_MALWARE\_LIST\_TRUNCATED\_EXIT**Message Meaning:** External malware list is no longer truncated**Type:** Event**Category:** SYSTEM**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 47203 - LOG\_ID\_ENTER\_BYPASS

**Message ID:** 47203

**Message Description:** LOG\_ID\_ENTER\_BYPASS

**Message Meaning:** Bypass ports pair entered bypass mode

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 47204 - LOG\_ID\_EXIT\_BYPASS

**Message ID:** 47204

**Message Description:** LOG\_ID\_EXIT\_BYPASS

**Message Meaning:** Bypass ports pair exited bypass mode

**Type:** Event

**Category:** SYSTEM

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 48000 - LOG\_ID\_WAD\_SSL\_RCV\_HS

**Message ID:** 48000

**Message Description:** LOG\_ID\_WAD\_SSL\_RCV\_HS

**Message Meaning:** SSL handshake received

**Type:** Event

**Category:** WAD

**Severity:** Debug

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
handshake	Handshake	string	32

## 48001 - LOG\_ID\_WAD\_SSL\_RCV\_WRG\_HS

**Message ID:** 48001

**Message Description:** LOG\_ID\_WAD\_SSL\_RCV\_WRG\_HS

**Message Meaning:** SSL handshake message incorrect

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65

## 48002 - LOG\_ID\_WAD\_SSL\_SENT\_HS

**Message ID:** 48002

**Message Description:** LOG\_ID\_WAD\_SSL\_SENT\_HS

**Message Meaning:** SSL handshake sent

**Type:** Event

**Category:** WAD

**Severity:** Debug

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32



Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
handshake	Handshake	string	32

## 48003 - LOG\_ID\_WAD\_SSL\_WRG\_HS\_LEN

**Message ID:** 48003

**Message Description:** LOG\_ID\_WAD\_SSL\_WRG\_HS\_LEN

**Message Meaning:** SSL handshake length invalid

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
handshake	Handshake	string	32

## 48004 - LOG\_ID\_WAD\_SSL\_RCV\_CCS

**Message ID:** 48004

**Message Description:** LOG\_ID\_WAD\_SSL\_RCV\_CCS

**Message Meaning:** SSL ChangeCipherSpec received

**Type:** Event

**Category:** WAD

**Severity:** Debug

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65

## 48005 - LOG\_ID\_WAD\_SSL\_RSA\_DH\_FAIL

**Message ID:** 48005

**Message Description:** LOG\_ID\_WAD\_SSL\_RSA\_DH\_FAIL

**Message Meaning:** RSA verification of Diffie-Hellman parameters failed

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

Log Field Name	Description	Data Type	Length
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65

## 48006 - LOG\_ID\_WAD\_SSL\_SENT\_CCS

**Message ID:** 48006

**Message Description:** LOG\_ID\_WAD\_SSL\_SENT\_CCS

**Message Meaning:** SSL ChangeCipherSpec sent

**Type:** Event

**Category:** WAD

**Severity:** Debug

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10

Log Field Name	Description	Data Type	Length
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65

## 48007 - LOG\_ID\_WAD\_SSL\_BAD\_HASH

**Message ID:** 48007

**Message Description:** LOG\_ID\_WAD\_SSL\_BAD\_HASH

**Message Meaning:** SSL Finished hash mismatch

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
ssllocal	SSL message	string	76
sslremote	SSL message	string	76

## 48009 - LOG\_ID\_WAD\_SSL\_DECRY\_FAIL

**Message ID:** 48009

**Message Description:** LOG\_ID\_WAD\_SSL\_DECRY\_FAIL

**Message Meaning:** SSL decryption failed

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5

Log Field Name	Description	Data Type	Length
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
reason	Reason	string	256

## 48011 - LOG\_ID\_WAD\_SSL\_LESS\_MINOR

**Message ID:** 48011

**Message Description:** LOG\_ID\_WAD\_SSL\_LESS\_MINOR

**Message Meaning:** SSL minor version less than configured minimum value

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39

Log Field Name	Description	Data Type	Length
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65

## 48013 - LOG\_ID\_WAD\_SSL\_NOT\_SUPPORT\_CS

**Message ID:** 48013

**Message Description:** LOG\_ID\_WAD\_SSL\_NOT\_SUPPORT\_CS

**Message Meaning:** SSL Cipher Suites not supported

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65



## 48016 - LOG\_ID\_WAD\_SSL\_HS\_FIN

**Message ID:** 48016

**Message Description:** LOG\_ID\_WAD\_SSL\_HS\_FIN

**Message Meaning:** SSL handshake completed

**Type:** Event

**Category:** WAD

**Severity:** Debug

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65

## 48017 - LOG\_ID\_WAD\_SSL\_HS\_TOO\_LONG

**Message ID:** 48017

**Message Description:** LOG\_ID\_WAD\_SSL\_HS\_TOO\_LONG

**Message Meaning:** SSL handshake too long

**Type:** Event**Category:** WAD**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
handshake	Handshake	string	32

## 48019 - LOG\_ID\_WAD\_SSL\_SENT\_ALERT

**Message ID:** 48019**Message Description:** LOG\_ID\_WAD\_SSL\_SENT\_ALERT**Message Meaning:** SSL alert sent**Type:** Event**Category:** WAD**Severity:** Debug

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
alert	Alert ID	string	256
desc	Description	string	128

## 48023 - LOG\_ID\_WAD\_SSL\_RCV\_ALERT

**Message ID:** 48023

**Message Description:** LOG\_ID\_WAD\_SSL\_RCV\_ALERT

**Message Meaning:** SSL alert received

**Type:** Event

**Category:** WAD

**Severity:** Debug

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
alert	Alert ID	string	256
desc	Description	string	128

## 48027 - LOG\_ID\_WAD\_SSL\_INVALID\_CONT\_TYPE

**Message ID:** 48027

**Message Description:** LOG\_ID\_WAD\_SSL\_INVALID\_CONT\_TYPE

**Message Meaning:** SSL Content Type invalid

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65

## 48029 - LOG\_ID\_WAD\_SSL\_BAD\_CCS\_LEN

**Message ID:** 48029

**Message Description:** LOG\_ID\_WAD\_SSL\_BAD\_CCS\_LEN

**Message Meaning:** SSL ChangeCipherSpec length invalid

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65

## 48031 - LOG\_ID\_WAD\_SSL\_BAD\_DH

**Message ID:** 48031

**Message Description:** LOG\_ID\_WAD\_SSL\_BAD\_DH

**Message Meaning:** SSL Diffie-Hellman value invalid

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16

Log Field Name	Description	Data Type	Length
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65

## 48032 - LOG\_ID\_WAD\_SSL\_PUB\_KEY\_TOO\_BIG

**Message ID:** 48032

**Message Description:** LOG\_ID\_WAD\_SSL\_PUB\_KEY\_TOO\_BIG

**Message Meaning:** Certificate's public key too long

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65

## 48034 - LOG\_ID\_WAD\_SSL\_SERVER\_KEY\_HASH\_ALGORITHM\_MISMATCH

**Message ID:** 48034

**Message Description:** LOG\_ID\_WAD\_SSL\_SERVER\_KEY\_HASH\_ALGORITHM\_MISMATCH

**Message Meaning:** Server Key Exchange hash algorithm mismatch

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32



Log Field Name	Description	Data Type	Length
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
received		uint8	3

## 48035 - LOG\_ID\_WAD\_SSL\_SERVER\_KEY\_SIGNATURE\_ALGORITHM\_MISMATCH

**Message ID:** 48035

**Message Description:** LOG\_ID\_WAD\_SSL\_SERVER\_KEY\_SIGNATURE\_ALGORITHM\_MISMATCH

**Message Meaning:** Server Key Exchange signature algorithm mismatch

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
expectedsignature		uint8	3
receivedsignature		uint8	3

## 48038 - LOG\_ID\_WAD\_SSL\_RCV\_FATAL\_ALERT

**Message ID:** 48038

**Message Description:** LOG\_ID\_WAD\_SSL\_RCV\_FATAL\_ALERT

**Message Meaning:** SSL Fatal Alert received

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
alert	Alert ID	string	256
desc	Description	string	128

## 48039 - LOG\_ID\_WAD\_SSL\_SENT\_FATAL\_ALERT

**Message ID:** 48039

**Message Description:** LOG\_ID\_WAD\_SSL\_SENT\_FATAL\_ALERT

**Message Meaning:** SSL fatal alert sent

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
action	Policy Action	string	65
alert	Alert ID	string	256
desc	Description	string	128

## 48101 - LOG\_ID\_WAD\_AUTH\_FAIL\_PSK

**Message ID:** 48101

**Message Description:** LOG\_ID\_WAD\_AUTH\_FAIL\_PSK

**Message Meaning:** WAN Optimization peer PSK authentication failed

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
serial	Serial Number	uint32	10
authgrp	Authorization Group	string	36
host	Host Name	string	256

## 48102 - LOG\_ID\_WAD\_AUTH\_FAIL\_OTH

**Message ID:** 48102

**Message Description:** LOG\_ID\_WAD\_AUTH\_FAIL\_OTH

**Message Meaning:** WAN Optimization peer authentication failed

**Type:** Event

**Category:** WAD

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
logdesc	Log Description	string	4096
msg	Log Message	string	4096
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
serial	Serial Number	uint32	10
authgrp	Authorization Group	string	36
peer	Address type	string	36

## 48301 - LOG\_ID\_UNEXP\_APP\_TYPE

**Message ID:** 48301

**Message Description:** LOG\_ID\_UNEXP\_APP\_TYPE

**Message Meaning:** Unexpected application type for WAN Optimization

**Type:** Event

**Category:** WAD

**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
session_id	Session ID	uint32	10
policyid	Policy ID	uint32	10
srcip	Source IP	ip	39
srcport	Source port	uint16	5
dstip	Destination IP	ip	39
dstport	Destination Protocol Port	uint16	5
app-type	Application type	string	64

## 49002 - LOG\_ID\_VNP\_DPDK\_PRIMARY\_RESTART

**Message ID:** 49002

**Message Description:** LOG\_ID\_VNP\_DPDK\_PRIMARY\_RESTART

**Message Meaning:** VNP Primary restarted

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 49004 - LOGID\_EVENT\_HYPERV\_SRIOV\_SHOW\_UP

**Message ID:** 49004

**Message Description:** LOGID\_EVENT\_HYPERV\_SRIOV\_SHOW\_UP

**Message Meaning:** Hyper-V SR-IOV secondary hot plugged

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 49005 - LOGID\_EVENT\_HYPERV\_SRIOV\_DISAPPEAR

**Message ID:** 49005

**Message Description:** LOGID\_EVENT\_HYPERV\_SRIOV\_DISAPPEAR

**Message Meaning:** Hyper-V SR-IOV secondary hot unplugged

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8



Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 51000 - LOG\_ID\_NB\_TBL\_CHG

**Message ID:** 51000

**Message Description:** LOG\_ID\_NB\_TBL\_CHG

**Message Meaning:** Neighbor table changed

**Type:** Event

**Category:** ROUTER

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

Log Field Name	Description	Data Type	Length
msg	Log Message	string	4096
action	Policy Action	string	65
service	Name of Service	string	64
mac	MAC Address	string	17
src_int	Source Interface	string	64
srcip	Source IP	ip	39

## 52000 - LOG\_ID\_EVENT\_SECURITY\_AUDIT\_FABRIC\_SUMMARY

**Message ID:** 52000

**Message Description:** LOG\_ID\_EVENT\_SECURITY\_AUDIT\_FABRIC\_SUMMARY

**Message Meaning:** Security Rating summary

**Type:** Event

**Category:** SECURITY-RATING

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
auditid	Security Rating ID	uint64	20
audittime	Security Rating time	uint64	20
auditscore	Security Rating score	string	20
auditreporttype	Security Rating report type	string	20

Log Field Name	Description	Data Type	Length
criticalcount	Critical level threat count	int32	10
highcount	Security Rating result failed count for high severity	int32	10
mediumcount	Security Rating result failed count for medium severity	int32	10
lowcount	Security Rating result failed count for low severity	int32	10
passedcount	Security Rating result passed count	int32	10

## 52001 - LOG\_ID\_EVENT\_SECURITY\_AUDIT\_FABRIC\_CHANGE

**Message ID:** 52001

**Message Description:** LOG\_ID\_EVENT\_SECURITY\_AUDIT\_FABRIC\_CHANGE

**Message Meaning:** Security Rating result change

**Type:** Event

**Category:** SECURITY-RATING

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
auditid	Security Rating ID	uint64	20
audittime	Security Rating time	uint64	20
auditscore	Security Rating score	string	20
auditreporttype	Security Rating report type	string	20
criticalcount	Critical level threat count	int32	10

Log Field Name	Description	Data Type	Length
highcount	Security Rating result failed count for high severity	int32	10
mediumcount	Security Rating result failed count for medium severity	int32	10
lowcount	Security Rating result failed count for low severity	int32	10
passedcount	Security Rating result passed count	int32	10

## 53000 - LOG\_ID\_SDNC\_CONNECTED

**Message ID:** 53000

**Message Description:** LOG\_ID\_SDNC\_CONNECTED

**Message Meaning:** Connected to SDN server

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 53001 - LOG\_ID\_SDNC\_DISCONNECTED

**Message ID:** 53001

**Message Description:** LOG\_ID\_SDNC\_DISCONNECTED

**Message Meaning:** Disconnected from SDN server

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
user	User name of authenticated user	string	256
action	Policy Action	string	65
msg	Log Message	string	4096

## 53002 - LOG\_ID\_SDNC\_SUBSCRIBE

**Message ID:** 53002

**Message Description:** LOG\_ID\_SDNC\_SUBSCRIBE

**Message Meaning:** Dynamic SDN address channel opened

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 53003 - LOG\_ID\_SDNC\_UNSUBSCRIBE

**Message ID:** 53003

**Message Description:** LOG\_ID\_SDNC\_UNSUBSCRIBE

**Message Meaning:** Dynamic SDN address channel closed

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 53100 - LOG\_ID\_VPN\_OCVPN\_REGISTERED

**Message ID:** 53100

**Message Description:** LOG\_ID\_VPN\_OCVPN\_REGISTERED

**Message Meaning:** Overlay Controller VPN registered

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
status	Status	string	23

## 53101 - LOG\_ID\_VPN\_OCVPN\_UNREGISTERED

**Message ID:** 53101

**Message Description:** LOG\_ID\_VPN\_OCVPN\_UNREGISTERED

**Message Meaning:** Overlay Controller VPN unregistered

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10

Log Field Name	Description	Data Type	Length
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
status	Status	string	23

## 53102 - LOG\_ID\_VPN\_OCVPN\_COMM\_ESTABLISHED

**Message ID:** 53102

**Message Description:** LOG\_ID\_VPN\_OCVPN\_COMM\_ESTABLISHED

**Message Meaning:** Overlay Controller VPN server communication established

**Type:** Event

**Category:** VPN

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20



Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
status	Status	string	23

## 53103 - LOG\_ID\_VPN\_OCVPN\_COMM\_ERROR

**Message ID:** 53103

**Message Description:** LOG\_ID\_VPN\_OCVPN\_COMM\_ERROR

**Message Meaning:** Overlay Controller VPN server communication error

**Type:** Event

**Category:** VPN

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
status	Status	string	23

## 53104 - LOG\_ID\_VPN\_OCVPN\_DNS\_ERROR

**Message ID:** 53104

**Message Description:** LOG\_ID\_VPN\_OCVPN\_DNS\_ERROR

**Message Meaning:** Overlay Controller VPN DNS error

**Type:** Event**Category:** VPN**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
status	Status	string	23

## 53105 - LOG\_ID\_VPN\_OCVPN\_ROUTE\_ERROR

**Message ID:** 53105**Message Description:** LOG\_ID\_VPN\_OCVPN\_ROUTE\_ERROR**Message Meaning:** Overlay Controller VPN routing error**Type:** Event**Category:** VPN**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
status	Status	string	23

## 53200 - LOG\_ID\_CONNECTOR\_OBJECT\_ADD

**Message ID:** 53200

**Message Description:** LOG\_ID\_CONNECTOR\_OBJECT\_ADD

**Message Meaning:** Dynamic address added

**Type:** Event

**Category:** CONNECTOR

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
fctemssn		string	16
addr	IP Address	string	80

Log Field Name	Description	Data Type	Length
cfgobj	Configuration object	string	256
action	Policy Action	string	65
cldobjid		string	128
netid		string	128
msg	Log Message	string	4096

## 53201 - LOG\_ID\_CONNECTOR\_OBJECT\_REMOVE

**Message ID:** 53201

**Message Description:** LOG\_ID\_CONNECTOR\_OBJECT\_REMOVE

**Message Meaning:** Dynamic address removed

**Type:** Event

**Category:** CONNECTOR

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
fctemssn		string	16
addr	IP Address	string	80
cfgobj	Configuration object	string	256
action	Policy Action	string	65
cldobjid		string	128

Log Field Name	Description	Data Type	Length
netid		string	128
msg	Log Message	string	4096

## 53202 - LOG\_ID\_CONNECTOR\_API\_FAILED

**Message ID:** 53202

**Message Description:** LOG\_ID\_CONNECTOR\_API\_FAILED

**Message Meaning:** SDN Connector API failed

**Type:** Event

**Category:** CONNECTOR

**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
fctemssn		string	16
addr	IP Address	string	80
msg	Log Message	string	4096

## 53203 - LOG\_ID\_CONNECTOR\_OBJECT\_UPDATE

**Message ID:** 53203

**Message Description:** LOG\_ID\_CONNECTOR\_OBJECT\_UPDATE

**Message Meaning:** Dynamic address updated

**Type:** Event

**Category:** CONNECTOR**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
fctemssn		string	16
addr	IP Address	string	80
msg	Log Message	string	4096

## 53204 - LOG\_ID\_CONNECTOR\_OBJECT\_CANT\_ADD

**Message ID:** 53204**Message Description:** LOG\_ID\_CONNECTOR\_OBJECT\_CANT\_ADD**Message Meaning:** Dynamic address can't be added**Type:** Event**Category:** CONNECTOR**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
fctemssn		string	16
addr	IP Address	string	80
msg	Log Message	string	4096

## 53205 - LOG\_ID\_CONNECTOR\_OBJECT\_CANT\_REMOVE

**Message ID:** 53205

**Message Description:** LOG\_ID\_CONNECTOR\_OBJECT\_CANT\_REMOVE

**Message Meaning:** Dynamic address can't be removed

**Type:** Event

**Category:** CONNECTOR

**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
fctemssn		string	16
addr	IP Address	string	80
msg	Log Message	string	4096

## 53300 - LOG\_ID\_VNE\_PRO\_UPDATE\_COMPLETED

**Message ID:** 53300

**Message Description:** LOG\_ID\_VNE\_PRO\_UPDATE\_COMPLETED

**Message Meaning:** VNE provision server update completed

**Type:** Event

**Category:** SYSTEM

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
server	Server IP Address	string	64
hostname	Hostname	string	128

## 53301 - LOG\_ID\_VNE\_PRO\_UPDATE\_FAILED

**Message ID:** 53301

**Message Description:** LOG\_ID\_VNE\_PRO\_UPDATE\_FAILED

**Message Meaning:** VNE provision server update failed

**Type:** Event

**Category:** SYSTEM

**Severity:** Information



Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096
error	Error Reason for Log Upload to Forticloud	string	256
server	Server IP Address	string	64
hostname	Hostname	string	128

## 53311 - LOG\_ID\_NPU\_PER\_MAPPING\_ALLOCATION

**Message ID:** 53311

**Message Description:** LOG\_ID\_NPU\_PER\_MAPPING\_ALLOCATION

**Message Meaning:** Resource per mapping allocation

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096

## 53312 - LOG\_ID\_NPD\_INFO

**Message ID:** 53312

**Message Description:** LOG\_ID\_NPD\_INFO

**Message Meaning:** NPD INFO

**Type:** Event

**Category:** SYSTEM

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 53313 - LOG\_ID\_NPD\_WARNING

**Message ID:** 53313

**Message Description:** LOG\_ID\_NPD\_WARNING

**Message Meaning:** NPD WARNING MSG

**Type:** Event**Category:** SYSTEM**Severity:** Warning

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## 53314 - LOG\_ID\_NPD\_ERROR

**Message ID:** 53314**Message Description:** LOG\_ID\_NPD\_ERROR**Message Meaning:** NPD ERROR MSG**Type:** Event**Category:** SYSTEM**Severity:** Error

Log Field Name	Description	Data Type	Length
date	Date	string	10
time	Time	string	8
logid	Log ID	string	10
type	Log Type	string	16
subtype	Log Subtype	string	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
vd	Virtual Domain Name	string	32
eventtime	Event time	uint64	20
tz	Time zone	string	5
logdesc	Log Description	string	4096
msg	Log Message	string	4096

## FILE-FILTER

### 64000 - LOG\_ID\_FILE\_FILTER\_BLOCK

**Message ID:** 64000

**Message Description:** LOG\_ID\_FILE\_FILTER\_BLOCK

**Message Meaning:** File was blocked by file filter

**Type:** FILE-FILTER

**Category:** FILE-FILTER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action		string	20
agent		string	64
attachment		string	3
authserver		string	64
cc		string	512
date		string	10
devid		string	16
direction		string	8
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventtime		uint64	20

Log Field Name	Description	Data Type	Length
eventtype		string	32
fctuid		string	32
filename		string	256
filesize		uint64	10
filetype		string	23
filtername		string	32
forwardedfor		string	128
from		string	128
group		string	64
hostname		string	256
level		string	11
logid		string	10
matchfilename		string	256
matchfiletype		string	23
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
rawdata		string	1024
recipient		string	512
sender		string	128
service		string	36
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrold		string	10
srcip		ip	39
srcport		uint16	5
subject		string	256
subservice		string	16

Log Field Name	Description	Data Type	Length
subtype		string	20
time		string	8
to		string	512
trueclntip		ip	39
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
url		string	512
user		string	256
vd		string	32
vrf		uint8	3

## 64001 - LOG\_ID\_FILE\_FILTER\_LOG

**Message ID:** 64001

**Message Description:** LOG\_ID\_FILE\_FILTER\_LOG

**Message Meaning:** File was detected by file filter

**Type:** FILE-FILTER

**Category:** FILE-FILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action		string	20
agent		string	64
attachment		string	3
authserver		string	64
cc		string	512
date		string	10
devid		string	16
direction		string	8
dstintf		string	32

Log Field Name	Description	Data Type	Length
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
filename		string	256
filesize		uint64	10
filetype		string	23
filtername		string	32
forwardedfor		string	128
from		string	128
group		string	64
hostname		string	256
level		string	11
logid		string	10
matchfilename		string	256
matchfiletype		string	23
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
rawdata		string	1024
recipient		string	512
sender		string	128
service		string	36
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10

Log Field Name	Description	Data Type	Length
srcip		ip	39
srcport		uint16	5
subject		string	256
subservice		string	16
subtype		string	20
time		string	8
to		string	512
trueclntip		ip	39
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
url		string	512
user		string	256
vd		string	32
vrf		uint8	3

## GTP

### 41216 - LOGID\_GTP\_FORWARD

**Message ID:** 41216

**Message Description:** LOGID\_GTP\_FORWARD

**Message Meaning:** GTP forward

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
c-gsn	Control Plane GSN	ip	39
cgsn6		ip	39



Log Field Name	Description	Data Type	Length
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
dtlexp	Detailed Explanation	string	64
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
ietype	Malformed GTP IE number	uint8	3
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
logid	Log ID	string	10
msg-type	Message Type	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
nsapi	Netscape Server Application Programming Interface	uint8	3
profile	Profile Name	string	64
rai	Routing Area Identifier	string	32
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
seqnum	GTP packet sequence number	uint32	10
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8

Log Field Name	Description	Data Type	Length
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
u-gsn	User Plane GSN	ip	39
ugsn6		ip	39
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64

## 41217 - LOGID\_GTP\_DENY

**Message ID:** 41217

**Message Description:** LOGID\_GTP\_DENY

**Message Meaning:** GTP deny

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
c-gsn	Control Plane GSN	ip	39
cgsn6		ip	39
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
dtlexp	Detailed Explanation	string	64
end-usr-address	End user IP Address	ip	39

Log Field Name	Description	Data Type	Length
endusraddress6		ip	39
eventtime	Event time line	uint64	20
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
ietype	Malformed GTP IE number	uint8	3
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
logid	Log ID	string	10
msg-type	Message Type	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
nsapi	Netscape Server Application Programming Interface	uint8	3
profile	Profile Name	string	64
rai	Routing Area Identifier	string	32
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
seqnum	GTP packet sequence number	uint32	10
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
u-gsn	User Plane GSN	ip	39

Log Field Name	Description	Data Type	Length
ugsn6		ip	39
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64

## 41218 - LOGID\_GTP\_RATE\_LIMIT

**Message ID:** 41218

**Message Description:** LOGID\_GTP\_RATE\_LIMIT

**Message Meaning:** GTP rate limit

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
c-gsn	Control Plane GSN	ip	39
cgsn6		ip	39
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
dtlexp	Detailed Explanation	string	64
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
ietype	Malformed GTP IE number	uint8	3

Log Field Name	Description	Data Type	Length
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
logid	Log ID	string	10
msg-type	Message Type	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
nsapi	Netscape Server Application Programming Interface	uint8	3
profile	Profile Name	string	64
rai	Routing Area Identifier	string	32
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
seqnum	GTP packet sequence number	uint32	10
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
u-gsn	User Plane GSN	ip	39
ugsn6		ip	39
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64

## 41219 - LOGID\_GTP\_STATE\_INVALID

**Message ID:** 41219

**Message Description:** LOGID\_GTP\_STATE\_INVALID

**Message Meaning:** GTP state invalid

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
c-gsn	Control Plane GSN	ip	39
cgsn6		ip	39
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
dtlexp	Detailed Explanation	string	64
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
ietype	Malformed GTP IE number	uint8	3
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
logid	Log ID	string	10
msg-type	Message Type	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16

Log Field Name	Description	Data Type	Length
nsapi	Netscape Server Application Programming Interface	uint8	3
profile	Profile Name	string	64
rai	Routing Area Identifier	string	32
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
seqnum	GTP packet sequence number	uint32	10
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
u-gsn	User Plane GSN	ip	39
ugsn6		ip	39
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64

## 41220 - LOGID\_GTP\_TUNNEL\_LIMIT

**Message ID:** 41220

**Message Description:** LOGID\_GTP\_TUNNEL\_LIMIT

**Message Meaning:** Tunnel limit GTP message. These messages occur only when the maximum number of GTP tunnels is reached. No new tunnels are created when the maximum number is reached

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
c-gsn	Control Plane GSN	ip	39
cgsn6		ip	39
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
dtlexp	Detailed Explanation	string	64
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
ietype	Malformed GTP IE number	uint8	3
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
logid	Log ID	string	10
msg-type	Message Type	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
nsapi	Netscape Server Application Programming Interface	uint8	3
profile	Profile Name	string	64
rai	Routing Area Identifier	string	32
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
seqnum	GTP packet sequence number	uint32	10
srcport	Source Port	uint16	5



Log Field Name	Description	Data Type	Length
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
u-gsn	User Plane GSN	ip	39
ugsn6		ip	39
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64

## 41221 - LOGID\_GTP\_TRAFFIC\_COUNT

**Message ID:** 41221

**Message Description:** LOGID\_GTP\_TRAFFIC\_COUNT

**Message Meaning:** Statistic summary information when the GTP tunnel is being torn down

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
date	Date	string	10
devid	Device ID	string	16
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20

Log Field Name	Description	Data Type	Length
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
linked-nsapi	Linked Netscape Server Application Programming Interface	uint8	3
logid	Log ID	string	10
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
nsapi	Netscape Server Application Programming Interface	uint8	3
profile	Profile Name	string	64
rai	Routing Area Identifier	string	32
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64
c-bytes	Control Plane Data Bytes	uint64	20
c-ggsn	Control Plane GGSN IP Address	ip	39
c-ggsn-teid	Control Plane GGSN Tunnel Endpoint Identifier	uint32	10
c-pkts	Control Plane Packets	uint64	20
c-sgsn	Control Plane SGSN IP Address	ip	39
c-sgsn-teid	Control Plane SGSN Tunnel Endpoint Identifier	uint32	10
cggsn6		ip	39

Log Field Name	Description	Data Type	Length
csgsn6		ip	39
duration	Tunnel duration	uint32	10
u-bytes	User Plane Data Bytes	uint64	20
u-ggsn	User plane ggsn IP address	ip	39
u-ggsn-teid	User plane ggsn teid	uint32	10
u-pkts	User Plane Packets	uint64	20
u-sgsn	User plane sgsn IP address	ip	39
u-sgsn-teid	User plane sgsn tunnel endpoint identifier	uint32	10
uggsn6		ip	39
usgsn6		ip	39

## 41222 - LOGID\_GTP\_USER\_DATA

**Message ID:** 41222

**Message Description:** LOGID\_GTP\_USER\_DATA

**Message Meaning:** GTP user data

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
date	Date	string	10
devid	Device ID	string	16
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20
from	From	ip	128
from6		ip	39
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
logid	Log ID	string	10

Log Field Name	Description	Data Type	Length
profile	Profile Name	string	64
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
vd	Virtual Domain Name	string	32
version	Version	uint32	64
user_data	User traffic content inside GTP-U tunnel	string	256

## 41223 - LOGID\_GTPV2\_FORWARD

**Message ID:** 41223

**Message Description:** LOGID\_GTPV2\_FORWARD

**Message Meaning:** GTPv2 forward message

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
dtlexp	Detailed Explanation	string	64
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20

Log Field Name	Description	Data Type	Length
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
ietype	Malformed GTP IE number	uint8	3
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
logid	Log ID	string	10
msg-type	Message Type	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
profile	Profile Name	string	64
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
seqnum	GTP packet sequence number	uint32	10
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64
cpaddr	Control Plane Address (either downlink or uplink)	ip	39

Log Field Name	Description	Data Type	Length
cpaddr6		ip	39
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64

## 41224 - LOGID\_GTPV2\_DENY

**Message ID:** 41224

**Message Description:** LOGID\_GTPV2\_DENY

**Message Meaning:** GTPv2 deny message

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
dtlexp	Detailed Explanation	string	64
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
ietype	Malformed GTP IE number	uint8	3
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
logid	Log ID	string	10
msg-type	Message Type	uint8	3

Log Field Name	Description	Data Type	Length
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
profile	Profile Name	string	64
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
seqnum	GTP packet sequence number	uint32	10
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64
cpaddr	Control Plane Address (either downlink or uplink)	ip	39
cpaddr6		ip	39
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64

## 41225 - LOGID\_GTPV2\_RATE\_LIMIT

**Message ID:** 41225

**Message Description:** LOGID\_GTPV2\_RATE\_LIMIT

**Message Meaning:** GTPv2 rate limit message

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
dtlexp	Detailed Explanation	string	64
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
ietype	Malformed GTP IE number	uint8	3
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
logid	Log ID	string	10
msg-type	Message Type	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
profile	Profile Name	string	64
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
seqnum	GTP packet sequence number	uint32	10
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39



Log Field Name	Description	Data Type	Length
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64
cpaddr	Control Plane Address (either downlink or uplink)	ip	39
cpaddr6		ip	39
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64

## 41226 - LOGID\_GTPV2\_STATE\_INVALID

**Message ID:** 41226

**Message Description:** LOGID\_GTPV2\_STATE\_INVALID

**Message Meaning:** GTPv2 state invalid message

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
dtlexp	Detailed Explanation	string	64
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20

Log Field Name	Description	Data Type	Length
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
ietype	Malformed GTP IE number	uint8	3
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
logid	Log ID	string	10
msg-type	Message Type	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
profile	Profile Name	string	64
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
seqnum	GTP packet sequence number	uint32	10
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64
cpaddr	Control Plane Address (either downlink or uplink)	ip	39

Log Field Name	Description	Data Type	Length
cpaddr6		ip	39
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64

## 41227 - LOGID\_GTPV2\_TUNNEL\_LIMIT

**Message ID:** 41227

**Message Description:** LOGID\_GTPV2\_TUNNEL\_LIMIT

**Message Meaning:** Tunnel limit GTP (version 2) message

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
dtlexp	Detailed Explanation	string	64
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
ietype	Malformed GTP IE number	uint8	3
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
logid	Log ID	string	10
msg-type	Message Type	uint8	3

Log Field Name	Description	Data Type	Length
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
profile	Profile Name	string	64
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
seqnum	GTP packet sequence number	uint32	10
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64
cpaddr	Control Plane Address (either downlink or uplink)	ip	39
cpaddr6		ip	39
cpteid	Control Plane teid (either downlink or uplink)	uint32	10
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64

## 41228 - LOGID\_GTPV2\_TRAFFIC\_COUNT

**Message ID:** 41228

**Message Description:** LOGID\_GTPV2\_TRAFFIC\_COUNT

**Message Meaning:** Statistic summary information when the GTPv2 tunnel is being torn down

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
date	Date	string	10
devid	Device ID	string	16
end-usr-address	End user IP Address	ip	39
endusraddress6		ip	39
eventtime	Event time line	uint64	20
imei-sv	IMEI(International Mobile Equipment Identity) Software Version	string	32
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
logid	Log ID	string	10
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
profile	Profile Name	string	64
rat-type	Radio Access Technology type	string	7
selection	APN selection, which is one IE in gtp packet	string	14
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
uli	User Location Information	string	120
ulimcc		uint16	3
ulimnc		uint16	3
vd	Virtual Domain Name	string	32
version	Version	uint32	64
c-bytes	Control Plane Data Bytes	uint64	20
c-pkts	Control Plane Packets	uint64	20
duration	Tunnel duration	uint32	10
u-bytes	User Plane Data Bytes	uint64	20

Log Field Name	Description	Data Type	Length
u-pkts	User Plane Packets	uint64	20
snetwork	Source Network, it's a IE type in GTPv2 packet	string	64
cpdladdr	Control Plane Downlink IP Address	ip	39
cpdladdr6		ip	39
cpdlisraddr	Control Plane ISR Downlink IP Address	ip	39
cpdlisraddr6		ip	39
cpdlisrteid	control plane ISR downlink tunnel endpoint identifier	uint32	10
cpdlteid	control plane downlink tunnel endpoint identifier	uint32	10
cpuladdr	control plane uplink IP address	ip	39
cpuladdr6		ip	39
cpulteid	control plane uplink teid	uint32	10

## 41229 - LOGID\_GTPU\_FORWARD

**Message ID:** 41229

**Message Description:** LOGID\_GTPU\_FORWARD

**Message Meaning:** GTPU forward message

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5
eventtime	Event time line	uint64	20
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
imsi	International mobile subscriber ID	string	16

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
logid	Log ID	string	10
msg-type	Message Type	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
profile	Profile Name	string	64
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
vd	Virtual Domain Name	string	32
version	Version	uint32	64

## 41230 - LOGID\_GTPU\_DENY

**Message ID:** 41230

**Message Description:** LOGID\_GTPU\_DENY

**Message Meaning:** GTPU deny message

**Type:** GTP

**Category:** GTP-ALL

**Severity:** Information

Log Field Name	Description	Data Type	Length
apn	Access Point Name	string	128
date	Date	string	10
deny_cause	Deny Cause	string	25
devid	Device ID	string	16
dstport	Destination Port	uint16	5

Log Field Name	Description	Data Type	Length
eventtime	Event time line	uint64	20
from	From	ip	128
from6		ip	39
headerteid	Tunnel Endpoint ID Header	uint32	10
imsi	International mobile subscriber ID	string	16
level	Log Level	string	11
logid	Log ID	string	10
msg-type	Message Type	uint8	3
msisdn	Mobile Subscriber Integrated Services Digital Network-Number (telephone # to a SIM card)	string	16
profile	Profile Name	string	64
srcport	Source Port	uint16	5
status	Status	string	23
subtype	Log Subtype	string	20
time	Time	string	8
to	To	ip	512
to6		ip	39
tunnel-idx	Tunnel serial number, internally assigned	uint32	10
type	Log Type	string	16
tz	Time zone	string	5
vd	Virtual Domain Name	string	32
version	Version	uint32	64

## ICAP

### 60000 - LOG\_ID\_ICAP\_SERVER\_ERROR

**Message ID:** 60000

**Message Description:** LOG\_ID\_ICAP\_SERVER\_ERROR

**Message Meaning:** Traffic blocked as it cannot be forwarded to ICAP Server.

**Type:** ICAP

**Category:** ICAP



**Severity:** Warning

Log Field Name	Description	Data Type	Length
action		string	17
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventtime		uint64	20
eventtype		string	32
level		string	11
logid		string	10
msg		string	4096
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
url		string	512
vd		string	32

## IPS

### 16384 - LOGID\_ATTCK\_SIGNATURE\_TCP\_UDP

**Message ID:** 16384

**Message Description:** LOGID\_ATTCK\_SIGNATURE\_TCP\_UDP

**Message Meaning:** Attack detected by UDP/TCP signature

**Type:** IPS

**Category:** SIGNATURE

**Severity:** Alert

Log Field Name	Description	Data Type	Length
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16
attack	Attack Name	string	256
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attackcontextid	Attack context ID / total	string	10
attackid	Attack ID	uint32	10
authserver	Authentication server for the user	string	64
craction	Action performed by Threat Weight	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Deivce ID	string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	IPS Event Type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
incidentserialno	Incident serial number	uint32	10
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message for the attack	string	518
policyid	Policy ID	uint32	10
profile	Profile name for IPS	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rawdataid		string	10
ref	URL of the FortiGuard IPS database entry for the attack.	string	4096
service	Service name	string	80
sessionid	Session ID	uint32	10
severity	Severity of the attack	string	8
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39

Log Field Name	Description	Data Type	Length
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 16385 - LOGID\_ATTCK\_SIGNATURE\_ICMP

**Message ID:** 16385

**Message Description:** LOGID\_ATTCK\_SIGNATURE\_ICMP

**Message Meaning:** Attack detected by ICMP signature

**Type:** IPS

**Category:** SIGNATURE

**Severity:** Alert

Log Field Name	Description	Data Type	Length
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16
attack	Attack Name	string	256
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attackcontextid	Attack context ID / total	string	10
attackid	Attack ID	uint32	10
authserver	Authentication server for the user	string	64
craction	Action performed by Threat Weight	uint32	10

Log Field Name	Description	Data Type	Length
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
eventtime	Time when detection occurred	uint64	20
eventtype	IPS Event Type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
incidentserialno	Incident serial number	uint32	10
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message for the attack	string	518
policyid	Policy ID	uint32	10
profile	Profile name for IPS	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rawdataid		string	10
ref	URL of the FortiGuard IPS database entry for the attack.	string	4096
service	Service name	string	80
sessionid	Session ID	uint32	10
severity	Severity of the attack	string	8
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcintf	Source Interface	string	64

Log Field Name	Description	Data Type	Length
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
subtype	Log Subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3
icmpcode	Destination Port of the ICMP message	string	6
icmpid	Source port of the ICMP message	string	8
icmptype	The type of ICMP message	string	6

## 16386 - LOGID\_ATTCK\_SIGNATURE\_OTHERS

**Message ID:** 16386

**Message Description:** LOGID\_ATTCK\_SIGNATURE\_OTHERS

**Message Meaning:** Attack detected by other signature

**Type:** IPS

**Category:** SIGNATURE

**Severity:** Alert

Log Field Name	Description	Data Type	Length
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16
attack	Attack Name	string	256
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attackcontextid	Attack context ID / total	string	10
attackid	Attack ID	uint32	10
authserver	Authentication server for the user	string	64
craction	Action performed by Threat Weight	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
eventtime	Time when detection occurred	uint64	20
eventtype	IPS Event Type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
incidentserialno	Incident serial number	uint32	10
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message for the attack	string	518

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	Profile name for IPS	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rawdataid		string	10
ref	URL of the FortiGuard IPS database entry for the attack.	string	4096
service	Service name	string	80
sessionid	Session ID	uint32	10
severity	Severity of the attack	string	8
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
subtype	Log Subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 16399 - LOGID\_ATTACK\_MALICIOUS\_URL

**Message ID:** 16399

**Message Description:** LOGID\_ATTACK\_MALICIOUS\_URL

**Message Meaning:** Attack detected by a malicious URL

**Type:** IPS



**Category:** MALICIOUS-URL**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16
attack	Attack Name	string	256
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attackcontextid	Attack context ID / total	string	10
authserver	Authentication server for the user	string	64
craction	Action performed by Threat Weight	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Deivce ID	string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	IPS Event Type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message for the attack	string	518

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	Profile name for IPS	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rawdataid		string	10
service	Service name	string	80
sessionid	Session ID	uint32	10
severity	Severity of the attack	string	8
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 16400 - LOGID\_ATTACK\_BOTNET\_WARNING

**Message ID:** 16400

**Message Description:** LOGID\_ATTACK\_BOTNET\_WARNING

**Message Meaning:** Botnet C&C Communication (warning)

**Type:** IPS**Category:** BOTNET**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16
attack	Attack Name	string	256
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attackcontextid	Attack context ID / total	string	10
attackid	Attack ID	uint32	10
authserver	Authentication server for the user	string	64
craction	Action performed by Threat Weight	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	IPS Event Type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
msg	Log message for the attack	string	518
policyid	Policy ID	uint32	10
profile	Profile name for IPS	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rawdataid		string	10
ref	URL of the FortiGuard IPS database entry for the attack.	string	4096
service	Service name	string	80
sessionid	Session ID	uint32	10
severity	Severity of the attack	string	8
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 16401 - LOGID\_ATTACK\_BOTNET\_NOTIF

**Message ID:** 16401

**Message Description:** LOGID\_ATTACK\_BOTNET\_NOTIF

**Message Meaning:** Botnet C&C Communication (notice)

**Type:** IPS

**Category:** BOTNET

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by IPS: detected - Attack is detected , but NOT blocked (similar to monitor) dropped - Silent packet blocked reset - Blocked and respond with Reset reset_client - Blocked and reset sent to the client reset_server - Blocked and reset sent to the server drop_session - Silent block pass_session - Session allowed clear_session - Session was removed /closed	string	16
attack	Attack Name	string	256
attackcontext	The trigger patterns and the packet data with base64 encoding	string	2048
attackcontextid	Attack context ID / total	string	10
attackid	Attack ID	uint32	10
authserver	Authentication server for the user	string	64
craction	Action performed by Threat Weight	uint32	10
crlevel	Client Reputation Level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Message/packets direction	string	8
dstintf	Destination Interface	string	64
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Time when detection occurred	uint64	20
eventtype	IPS Event Type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128

Log Field Name	Description	Data Type	Length
group	User group name	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message for the attack	string	518
policyid	Policy ID	uint32	10
profile	Profile name for IPS	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rawdataid		string	10
ref	URL of the FortiGuard IPS database entry for the attack.	string	4096
service	Service name	string	80
sessionid	Session ID	uint32	10
severity	Severity of the attack	string	8
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcintf	Source Interface	string	64
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz		string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## SSH

### 61000 - LOG\_ID\_SSH\_COMMAND\_BLOCK

**Message ID:** 61000

**Message Description:** LOG\_ID\_SSH\_COMMAND\_BLOCK

**Message Meaning:** SSH shell command is blocked

**Type:** SSH

**Category:** SSH-COMMAND

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17
channeletype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
command	Shell command	string	256
date	Date	string	10
devid	Device ID	string	16
direction	Direction of session	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event time	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	Group name for authentication	string	64
level	Log level	string	11
logid	Log ID	string	10
login	SSH login Name	string	128
policyid	Policy ID	uint32	10
profile	Full profile name	string	64

Log Field Name	Description	Data Type	Length
proto	Protocol number	uint8	3
sessionid	Session ID	uint32	10
severity	Severity level of shell command	string	8
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name for authentication	string	256
vd	Virtual Domain Name	string	32

## 61001 - LOG\_ID\_SSH\_COMMAND\_BLOCK\_ALERT

**Message ID:** 61001

**Message Description:** LOG\_ID\_SSH\_COMMAND\_BLOCK\_ALERT

**Message Meaning:** SSH shell command is blocked

**Type:** SSH

**Category:** SSH-COMMAND

**Severity:** Alert

Log Field Name	Description	Data Type	Length
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp, scp	string	15
command	Shell command	string	256



Log Field Name	Description	Data Type	Length
date	Date	string	10
devid	Device ID	string	16
direction	Direction of session	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event time	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	Group name for authentication	string	64
level	Log level	string	11
logid	Log ID	string	10
login	SSH login Name	string	128
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol number	uint8	3
sessionid	Session ID	uint32	10
severity	Severity level of shell command	string	8
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66

Log Field Name	Description	Data Type	Length
user	User name for authentication	string	256
vd	Virtual Domain Name	string	32

## 61002 - LOG\_ID\_SSH\_COMMAND\_PASS

**Message ID:** 61002

**Message Description:** LOG\_ID\_SSH\_COMMAND\_PASS

**Message Meaning:** SSH shell command is detected

**Type:** SSH

**Category:** SSH-COMMAND

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17
channeletype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp, scp	string	15
command	Shell command	string	256
date	Date	string	10
devid	Device ID	string	16
direction	Direction of session	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event time	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	Group name for authentication	string	64
level	Log level	string	11
logid	Log ID	string	10
login	SSH login Name	string	128

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol number	uint8	3
sessionid	Session ID	uint32	10
severity	Severity level of shell command	string	8
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name for authentication	string	256
vd	Virtual Domain Name	string	32

## 61003 - LOG\_ID\_SSH\_COMMAND\_PASS\_ALERT

**Message ID:** 61003

**Message Description:** LOG\_ID\_SSH\_COMMAND\_PASS\_ALERT

**Message Meaning:** SSH shell command is detected

**Type:** SSH

**Category:** SSH-COMMAND

**Severity:** Alert

Log Field Name	Description	Data Type	Length
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17

Log Field Name	Description	Data Type	Length
channeltype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
command	Shell command	string	256
date	Date	string	10
devid	Device ID	string	16
direction	Direction of session	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event time	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	Group name for authentication	string	64
level	Log level	string	11
logid	Log ID	string	10
login	SSH login Name	string	128
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol number	uint8	3
sessionid	Session ID	uint32	10
severity	Severity level of shell command	string	8
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz	Time zone	string	5

Log Field Name	Description	Data Type	Length
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name for authentication	string	256
vd	Virtual Domain Name	string	32

## 61010 - LOG\_ID\_SSH\_CHANNEL\_BLOCK

**Message ID:** 61010

**Message Description:** LOG\_ID\_SSH\_CHANNEL\_BLOCK

**Message Meaning:** SSH channel is blocked

**Type:** SSH

**Category:** SSH-CHANNEL

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17
channeletype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
command	Shell command	string	256
date	Date	string	10
devid	Device ID	string	16
direction	Direction of session	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event time	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	Group name for authentication	string	64
level	Log level	string	11

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
login	SSH login Name	string	128
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol number	uint8	3
sessionid	Session ID	uint32	10
severity	Severity level of shell command	string	8
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name for authentication	string	256
vd	Virtual Domain Name	string	32

## 61011 - LOG\_ID\_SSH\_CHANNEL\_PASS

**Message ID:** 61011

**Message Description:** LOG\_ID\_SSH\_CHANNEL\_PASS

**Message Meaning:** SSH channel is detected

**Type:** SSH

**Category:** SSH-CHANNEL

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the ssh-channel: passthrough - channel is allowed blocked - channel is blocked	string	17
channeletype	Type of Channel: x11, shell, exec, tcp-fprward, tun-forward, sftp. scp	string	15
command	Shell command	string	256
date	Date	string	10
devid	Device ID	string	16
direction	Direction of session	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Event time	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	Group name for authentication	string	64
level	Log level	string	11
logid	Log ID	string	10
login	SSH login Name	string	128
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol number	uint8	3
sessionid	Session ID	uint32	10
severity	Severity level of shell command	string	8
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20

Log Field Name	Description	Data Type	Length
time	Time	string	8
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated User	string	66
unauthusersource	Unauthenticated User Source	string	66
user	User name for authentication	string	256
vd	Virtual Domain Name	string	32

## SSL

### 62004 - LOG\_ID\_SSL\_EXEMPT\_ADDR

**Message ID:** 62004

**Message Description:** LOG\_ID\_SSL\_EXEMPT\_ADDR

**Message Meaning:** SSL connection is exempted based on address

**Type:** SSL

**Category:** SSL-EXEMPT

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action		string	20
cat		uint8	3
catdesc		string	64
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32



Log Field Name	Description	Data Type	Length
fctuid		string	32
group		string	64
hostname		string	256
level		string	11
logid		string	10
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## 62006 - LOG\_ID\_SSL\_EXEMPT\_WHITELIST

**Message ID:** 62006

**Message Description:** LOG\_ID\_SSL\_EXEMPT\_WHITELIST

**Message Meaning:** SSL connection is exempted based on whitelist

**Type:** SSL

**Category:** SSL-EXEMPT

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action		string	20
cat		uint8	3
catdesc		string	64
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64
hostname		string	256
level		string	11
logid		string	10
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8

Log Field Name	Description	Data Type	Length
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## 62007 - LOG\_ID\_SSL\_EXEMPT\_FTGD\_CATEGORY

**Message ID:** 62007

**Message Description:** LOG\_ID\_SSL\_EXEMPT\_FTGD\_CATEGORY

**Message Meaning:** SSL connection is exempted based on FortiGuard category rating

**Type:** SSL

**Category:** SSL-EXEMPT

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action		string	20
cat		uint8	3
catdesc		string	64
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64

Log Field Name	Description	Data Type	Length
hostname		string	256
level		string	11
logid		string	10
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## 62008 - LOG\_ID\_SSL\_EXEMPT\_LOCAL\_CATEGORY

**Message ID:** 62008

**Message Description:** LOG\_ID\_SSL\_EXEMPT\_LOCAL\_CATEGORY

**Message Meaning:** SSL connection is exempted based on local category rating

**Type:** SSL

**Category:** SSL-EXEMPT

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action		string	20
cat		uint8	3
catdesc		string	64
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64
hostname		string	256
level		string	11
logid		string	10
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8

Log Field Name	Description	Data Type	Length
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## 62009 - LOG\_ID\_SSL\_EXEMPT\_USER\_CATEGORY

**Message ID:** 62009

**Message Description:** LOG\_ID\_SSL\_EXEMPT\_USER\_CATEGORY

**Message Meaning:** SSL connection is exempted based on user category rating

**Type:** SSL

**Category:** SSL-EXEMPT

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action		string	20
cat		uint8	3
catdesc		string	64
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64

Log Field Name	Description	Data Type	Length
hostname		string	256
level		string	11
logid		string	10
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## 62100 - LOG\_ID\_SSL\_NEGOTIATION\_INSPECT

**Message ID:** 62100

**Message Description:** LOG\_ID\_SSL\_NEGOTIATION\_INSPECT

**Message Meaning:** Continue inspect the SSL connection

**Type:** SSL

**Category:** SSL-NEGOTIATION

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action		string	20
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64
hostname		string	256
level		string	11
logid		string	10
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5



Log Field Name	Description	Data Type	Length
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## 62101 - LOG\_ID\_SSL\_NEGOTIATION\_BLOCK

**Message ID:** 62101

**Message Description:** LOG\_ID\_SSL\_NEGOTIATION\_BLOCK

**Message Meaning:** SSL connection is blocked due to its SSL negotiation

**Type:** SSL

**Category:** SSL-NEGOTIATION

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action		string	20
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64
hostname		string	256
level		string	11
logid		string	10
msg		string	512

Log Field Name	Description	Data Type	Length
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## 62102 - LOG\_ID\_SSL\_NEGOTIATION\_BYPASS

**Message ID:** 62102

**Message Description:** LOG\_ID\_SSL\_NEGOTIATION\_BYPASS

**Message Meaning:** SSL connection is bypassed due to its SSL negotiation

**Type:** SSL

**Category:** SSL-NEGOTIATION

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action		string	20
date		string	10

Log Field Name	Description	Data Type	Length
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64
hostname		string	256
level		string	11
logid		string	10
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66

Log Field Name	Description	Data Type	Length
user		string	256
vd		string	32
vrf		uint8	3

## 62300 - LOG\_ID\_SSL\_ANOMALY\_CERT\_BLACKLISTED

**Message ID:** 62300

**Message Description:** LOG\_ID\_SSL\_ANOMALY\_CERT\_BLACKLISTED

**Message Meaning:** SSL connection is blocked due to the server certificate is blacklisted

**Type:** SSL

**Category:** SSL-ANOMALIES

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action		string	20
certdesc		string	64
certhash		string	40
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64
hostname		string	256
level		string	11
logid		string	10
msg		string	512

Log Field Name	Description	Data Type	Length
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## 62301 - LOG\_ID\_SSL\_ANOMALY\_CERT\_RESIGN\_TRUSTED

**Message ID:** 62301

**Message Description:** LOG\_ID\_SSL\_ANOMALY\_CERT\_RESIGN\_TRUSTED

**Message Meaning:** (null)

**Type:** SSL

**Category:** SSL-ANOMALIES

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action		string	20
certdesc		string	64

Log Field Name	Description	Data Type	Length
certhash		string	40
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64
hostname		string	256
level		string	11
logid		string	10
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5

Log Field Name	Description	Data Type	Length
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## 62302 - LOG\_ID\_SSL\_ANOMALY\_CERT\_RESIGN\_UNTRUSTED

**Message ID:** 62302

**Message Description:** LOG\_ID\_SSL\_ANOMALY\_CERT\_RESIGN\_UNTRUSTED

**Message Meaning:** (null)

**Type:** SSL

**Category:** SSL-ANOMALIES

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action		string	20
certdesc		string	64
certhash		string	40
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventssubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64
hostname		string	256
level		string	11

Log Field Name	Description	Data Type	Length
logid		string	10
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## 62303 - LOG\_ID\_SSL\_ANOMALY\_CERT\_BLOCKED

**Message ID:** 62303

**Message Description:** LOG\_ID\_SSL\_ANOMALY\_CERT\_BLOCKED

**Message Meaning:** (null)

**Type:** SSL

**Category:** SSL-ANOMALIES

**Severity:** Warning



Log Field Name	Description	Data Type	Length
action		string	20
certdesc		string	64
certhash		string	40
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64
hostname		string	256
level		string	11
logid		string	10
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8

Log Field Name	Description	Data Type	Length
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## 62304 - LOG\_ID\_SSL\_ANOMALY\_CERT\_SNI\_MISMATCHED

**Message ID:** 62304

**Message Description:** LOG\_ID\_SSL\_ANOMALY\_CERT\_SNI\_MISMATCHED

**Message Meaning:** (null)

**Type:** SSL

**Category:** SSL-ANOMALIES

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action		string	20
certdesc		string	64
certhash		string	40
date		string	10
devid		string	16
dstintf		string	32
dstintfrole		string	10
dstip		ip	39
dstport		uint16	5
eventsubtype		string	32
eventtime		uint64	20
eventtype		string	32
fctuid		string	32
group		string	64

Log Field Name	Description	Data Type	Length
hostname		string	256
level		string	11
logid		string	10
msg		string	512
policyid		uint32	10
profile		string	64
proto		uint8	3
service		string	5
sessionid		uint32	10
srcdomain		string	255
srcintf		string	32
srcintfrole		string	10
srcip		ip	39
srcport		uint16	5
subtype		string	20
time		string	8
type		string	16
tz		string	5
unauthuser		string	66
unauthusersource		string	66
user		string	256
vd		string	32
vrf		uint8	3

## Traffic

### 2 - LOG\_ID\_TRAFFIC\_ALLOW

**Message ID:** 2

**Message Description:** LOG\_ID\_TRAFFIC\_ALLOW

**Message Meaning:** Allowed traffic

**Type:** Traffic

**Category:** FORWARD**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64

Log Field Name	Description	Data Type	Length
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srcfamily		string	66
srchwvvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66

Log Field Name	Description	Data Type	Length
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

### 3 - LOG\_ID\_TRAFFIC\_DENY

**Message ID:** 3

**Message Description:** LOG\_ID\_TRAFFIC\_DENY

**Message Meaning:** Traffic violation

**Type:** Traffic

**Category:** FORWARD

**Severity:** Warning



Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66

Log Field Name	Description	Data Type	Length
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17

Log Field Name	Description	Data Type	Length
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66

Log Field Name	Description	Data Type	Length
srchwvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256

Log Field Name	Description	Data Type	Length
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 4 - LOG\_ID\_TRAFFIC\_OTHER\_START

**Message ID:** 4

**Message Description:** LOG\_ID\_TRAFFIC\_OTHER\_START

**Message Meaning:** Traffic other session start

**Type:** Traffic

**Category:** FORWARD

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39

Log Field Name	Description	Data Type	Length
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37

Log Field Name	Description	Data Type	Length
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17



Log Field Name	Description	Data Type	Length
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36

Log Field Name	Description	Data Type	Length
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 5 - LOG\_ID\_TRAFFIC\_OTHER\_ICMP\_ALLOW

**Message ID:** 5

**Message Description:** LOG\_ID\_TRAFFIC\_OTHER\_ICMP\_ALLOW

**Message Meaning:** Traffic allowed ICMP

**Type:** Traffic

**Category:** FORWARD

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64

Log Field Name	Description	Data Type	Length
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3

Log Field Name	Description	Data Type	Length
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20

Log Field Name	Description	Data Type	Length
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66

Log Field Name	Description	Data Type	Length
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 6 - LOG\_ID\_TRAFFIC\_OTHER\_ICMP\_DENY

**Message ID:** 6

**Message Description:** LOG\_ID\_TRAFFIC\_OTHER\_ICMP\_DENY

**Message Meaning:** Traffic denied ICMP

**Type:** Traffic

**Category:** FORWARD

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10

Log Field Name	Description	Data Type	Length
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32



Log Field Name	Description	Data Type	Length
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvdelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36

Log Field Name	Description	Data Type	Length
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5

Log Field Name	Description	Data Type	Length
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 7 - LOG\_ID\_TRAFFIC\_OTHER\_INVALID

**Message ID:** 7

**Message Description:** LOG\_ID\_TRAFFIC\_OTHER\_INVALID

**Message Meaning:** Traffic other invalid

**Type:** Traffic

**Category:** FORWARD

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66

Log Field Name	Description	Data Type	Length
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17

Log Field Name	Description	Data Type	Length
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
polycname	Policy name	string	36
policytype	Policy type	string	24
poluid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentedelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66

Log Field Name	Description	Data Type	Length
srchwvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256

Log Field Name	Description	Data Type	Length
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwplanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 8 - LOG\_ID\_TRAFFIC\_WANOPT

**Message ID:** 8

**Message Description:** LOG\_ID\_TRAFFIC\_WANOPT

**Message Meaning:** WAN optimization traffic

**Type:** Traffic

**Category:** FORWARD

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16



Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39

Log Field Name	Description	Data Type	Length
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37

Log Field Name	Description	Data Type	Length
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17

Log Field Name	Description	Data Type	Length
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36

Log Field Name	Description	Data Type	Length
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20
countapp	Number of App Ctrl logs associated with the session	uint32	10
countav	Number of AV logs associated with the session	uint32	10
countcifs		uint32	10
countdlp	Number of DLP logs associated with the session	uint32	10
countdns	Number of DNS Query logs associated with the session	uint32	10
countemail	Number of Email logs associated with the session	uint32	10
countff		uint32	10
counticap		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countssl		uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countweb	Number of Web Filter logs associated with the session	uint32	10

## 9 - LOG\_ID\_TRAFFIC\_WEBCACHE

**Message ID:** 9

**Message Description:** LOG\_ID\_TRAFFIC\_WEBCACHE

**Message Meaning:** Web cache traffic

**Type:** Traffic

**Category:** FORWARD

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66

Log Field Name	Description	Data Type	Length
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17

Log Field Name	Description	Data Type	Length
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66



Log Field Name	Description	Data Type	Length
srchwvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256

Log Field Name	Description	Data Type	Length
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20
countapp	Number of App Ctrl logs associated with the session	uint32	10
countav	Number of AV logs associated with the session	uint32	10
countcifs		uint32	10
countdlp	Number of DLP logs associated with the session	uint32	10
countdns	Number of DNS Query logs associated with the session	uint32	10
countemail	Number of Email logs associated with the session	uint32	10
countff		uint32	10
counticap		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countssl		uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countweb	Number of Web Filter logs associated with the session	uint32	10

## 10 - LOG\_ID\_TRAFFIC\_EXPLICIT\_PROXY

**Message ID:** 10

**Message Description:** LOG\_ID\_TRAFFIC\_EXPLICIT\_PROXY

**Message Meaning:** Explicit proxy traffic

**Type:** Traffic**Category:** FORWARD**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32

Log Field Name	Description	Data Type	Length
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20

Log Field Name	Description	Data Type	Length
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
polycyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentedelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64

Log Field Name	Description	Data Type	Length
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66

Log Field Name	Description	Data Type	Length
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20
countapp	Number of App Ctrl logs associated with the session	uint32	10
countav	Number of AV logs associated with the session	uint32	10
countcifs		uint32	10
countdlp	Number of DLP logs associated with the session	uint32	10
countdns	Number of DNS Query logs associated with the session	uint32	10
countemail	Number of Email logs associated with the session	uint32	10
countff		uint32	10
counticap		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countssl		uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countweb	Number of Web Filter logs associated with the session	uint32	10

## 11 - LOG\_ID\_TRAFFIC\_FAIL\_CONN

**Message ID:** 11

**Message Description:** LOG\_ID\_TRAFFIC\_FAIL\_CONN

**Message Meaning:** Failed connection attempts

**Type:** Traffic

**Category:** FORWARD

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10



Log Field Name	Description	Data Type	Length
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32

Log Field Name	Description	Data Type	Length
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
polycname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvdelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentedelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36

Log Field Name	Description	Data Type	Length
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5

Log Field Name	Description	Data Type	Length
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 12 - LOG\_ID\_TRAFFIC\_MULTICAST

**Message ID:** 12

**Message Description:** LOG\_ID\_TRAFFIC\_MULTICAST

**Message Meaning:** Multicast traffic

**Type:** Traffic

**Category:** MULTICAST

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66

Log Field Name	Description	Data Type	Length
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17

Log Field Name	Description	Data Type	Length
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentedelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66

Log Field Name	Description	Data Type	Length
srchwvvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256



Log Field Name	Description	Data Type	Length
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwplanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 13 - LOG\_ID\_TRAFFIC\_END\_FORWARD

**Message ID:** 13

**Message Description:** LOG\_ID\_TRAFFIC\_END\_FORWARD

**Message Meaning:** Forward traffic

**Type:** Traffic

**Category:** FORWARD

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39

Log Field Name	Description	Data Type	Length
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37

Log Field Name	Description	Data Type	Length
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17

Log Field Name	Description	Data Type	Length
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36

Log Field Name	Description	Data Type	Length
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20
countapp	Number of App Ctrl logs associated with the session	uint32	10
countav	Number of AV logs associated with the session	uint32	10
countcifs		uint32	10
countdlp	Number of DLP logs associated with the session	uint32	10
countdns	Number of DNS Query logs associated with the session	uint32	10
countemail	Number of Email logs associated with the session	uint32	10
countff		uint32	10
counticap		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countssl		uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countweb	Number of Web Filter logs associated with the session	uint32	10

## 14 - LOG\_ID\_TRAFFIC\_END\_LOCAL

**Message ID:** 14

**Message Description:** LOG\_ID\_TRAFFIC\_END\_LOCAL

**Message Meaning:** Local traffic

**Type:** Traffic

**Category:** LOCAL

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66

Log Field Name	Description	Data Type	Length
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17



Log Field Name	Description	Data Type	Length
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
polycyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentedelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66

Log Field Name	Description	Data Type	Length
srchwvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256

Log Field Name	Description	Data Type	Length
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwplanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 15 - LOG\_ID\_TRAFFIC\_START\_FORWARD

**Message ID:** 15

**Message Description:** LOG\_ID\_TRAFFIC\_START\_FORWARD

**Message Meaning:** Forward traffic session start

**Type:** Traffic

**Category:** FORWARD

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39

Log Field Name	Description	Data Type	Length
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37

Log Field Name	Description	Data Type	Length
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17

Log Field Name	Description	Data Type	Length
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36

Log Field Name	Description	Data Type	Length
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 16 - LOG\_ID\_TRAFFIC\_START\_LOCAL

**Message ID:** 16

**Message Description:** LOG\_ID\_TRAFFIC\_START\_LOCAL

**Message Meaning:** Local traffic session start

**Type:** Traffic

**Category:** LOCAL

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64



Log Field Name	Description	Data Type	Length
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3

Log Field Name	Description	Data Type	Length
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20

Log Field Name	Description	Data Type	Length
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66

Log Field Name	Description	Data Type	Length
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwplanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 17 - LOG\_ID\_TRAFFIC\_SNIFFER

**Message ID:** 17

**Message Description:** LOG\_ID\_TRAFFIC\_SNIFFER

**Message Meaning:** Sniffer traffic

**Type:** Traffic

**Category:** SNIFFER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application Name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
countapp	Number of App Ctrl logs associated with the session	uint32	10
countav	Number of AV logs associated with the session	uint32	10
countcifs		uint32	10

Log Field Name	Description	Data Type	Length
countdlp	Number of DLP logs associated with the session	uint32	10
countdns	Number of DNS Query logs associated with the session	uint32	10
countemail	Number of Email logs associated with the session	uint32	10
countff		uint32	10
counticap		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countssl		uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countweb	Number of Web Filter logs associated with the session	uint32	10
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66

Log Field Name	Description	Data Type	Length
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20

Log Field Name	Description	Data Type	Length
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64



Log Field Name	Description	Data Type	Length
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10

Log Field Name	Description	Data Type	Length
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 19 - LOG\_ID\_TRAFFIC\_BROADCAST

**Message ID:** 19

**Message Description:** LOG\_ID\_TRAFFIC\_BROADCAST

**Message Meaning:** Broadcast traffic

**Type:** Traffic

**Category:** MULTICAST

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10

Log Field Name	Description	Data Type	Length
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66

Log Field Name	Description	Data Type	Length
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10

Log Field Name	Description	Data Type	Length
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8

Log Field Name	Description	Data Type	Length
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 20 - LOG\_ID\_TRAFFIC\_STAT

**Message ID:** 20

**Message Description:** LOG\_ID\_TRAFFIC\_STAT

**Message Meaning:** Forward traffic statistics

**Type:** Traffic

**Category:** FORWARD**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64

Log Field Name	Description	Data Type	Length
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11



Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srcfamily		string	66
srchwvvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66

Log Field Name	Description	Data Type	Length
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 21 - LOG\_ID\_TRAFFIC\_SNIFFER\_STAT

**Message ID:** 21

**Message Description:** LOG\_ID\_TRAFFIC\_SNIFFER\_STAT

**Message Meaning:** Sniffer traffic statistics

**Type:** Traffic

**Category:** SNIFFER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application Name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66

Log Field Name	Description	Data Type	Length
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17

Log Field Name	Description	Data Type	Length
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
polycname	Policy name	string	36
policytype	Policy type	string	24
poluid	UUID of the Firewall Policy	string	37
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentedelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66

Log Field Name	Description	Data Type	Length
srchwvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256

Log Field Name	Description	Data Type	Length
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwplanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20

## 22 - LOG\_ID\_TRAFFIC\_UTM\_CORRELATION

**Message ID:** 22

**Message Description:** LOG\_ID\_TRAFFIC\_UTM\_CORRELATION

**Message Meaning:** Forward traffic for UTM correlation

**Type:** Traffic

**Category:** FORWARD

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	The status of the session: deny - Session was denied accept - Allowed Forward session start - Session starts (log message was created when the session was created) dns - DNS query return error ip-conn - Failed connection attempts close - Local-traffic session allowed timeout - Allowed session was timeout client-rst - Session reset by client server-rst - Session reset by server	string	16



Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	64
ap	Access Point name	string	36
app	Application name	string	96
appact	The security action from app control	string	16
appcat	Application category	string	64
appid	Application ID	uint32	10
applist	Application Control profile (name)	string	64
apprisk	Application Risk Level	string	16
apsn	Access Point serial number	string	36
authserver	Remote Authentication server	string	64
centralnatid	central-snat-map id	uint32	10
channel	WiFi Channel	uint32	10
comment	Customized policy comment	string	1024
craction	Action performed by Threat Weight	uint32	10
crlevel	Threat Weight level	string	10
crscore	Threat Weight score	uint32	10
date	Date	string	10
devid	Device Serial Number	string	16
devtype	Device Type	string	66
dstauthserver		string	32
dstcity		string	64
dstcountry	Country name for the destination IP	string	64
dstdevtype	Destination Device Type	string	66
dstfamily		string	66
dsthwvendor		string	66
dsthwversion		string	66
dstinetsvc	Internet service name for the destination	string	64
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39

Log Field Name	Description	Data Type	Length
dstmac	Destination Mac Address	string	17
dstname	Destination name	string	66
dstosname	Destination OS name	string	66
dstport	Destination Protocol Port Number	uint16	5
dstregion		string	64
dstreputation		uint32	10
dstserver	Destination Server	uint8	3
dstssid	Destination SSID	string	33
dstswversion		string	66
dstunauthuser		string	66
dstunauthusersource		string	66
dstuser		string	256
dstuuid	UUID of the Destination Address Object	string	37
duration	Duration of the session	uint32	10
eventtime	Epoch time in nanoseconds	uint64	20
fctuid	FortiClient UID	string	32
group	User group name	string	64
identifier		uint16	5
lanin	LAN incoming traffic in bytes	uint64	20
lanout	LAN outgoing traffic in bytes	uint64	20
level	Log Level	string	11
logid	Log ID	string	10
masterdstmac	Destination master MAC address	string	17
mastersrcmac	The master MAC address for a host that has multiple network interfaces	string	17
msg	Log message	string	64
osname	Name of the device's OS	string	66
policyid	Firewall Policy ID	uint32	10
policyname	Policy name	string	36
policytype	Policy type	string	24
poluuid	UUID of the Firewall Policy	string	37

Log Field Name	Description	Data Type	Length
proto	Protocol Number	uint8	3
radioband	Radio Band	string	64
rcvdbyte	Received Bytes	uint64	20
rcvddelta	Delta Received Bytes	uint64	20
rcvdpkt	Received Packets	uint32	10
sentbyte	Sent Bytes	uint64	20
sentdelta	Delta Sent Bytes	uint64	20
sentpkt	Sent Packets	uint32	10
service	Name of Service	string	80
sessionid	Session ID	uint32	10
shaperdroprcvdbyte	Received bytes dropped by shaper	uint32	10
shaperdropsentbyte	Sent bytes dropped by shaper	uint32	10
shaperperipdropbyte	Dropped bytes per IP by shaper	uint32	10
shaperperipname	Traffic shaper name (per IP)	string	36
shaperrcvdname	Traffic shaper name for received traffic	string	36
shapersentname	Traffic shaper name for sent traffic	string	36
shapingpolicyid	Shaping Policy ID	uint32	10
signal		int8	4
snr		int8	4
srccity		string	64
srccountry	Country name for Source IP	string	64
srcdomain		string	255
srcfamily		string	66
srchwvvendor		string	66
srchwversion		string	66
srcinetsvc	Internet service name for the source	string	64
srcintf	Source interface name	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP address	ip	39
srcmac	MAC address associated with the Source IP	string	17

Log Field Name	Description	Data Type	Length
srcname	Source name	string	66
srcport	Source protocol port number	uint16	5
srcregion		string	64
srcreputation		uint32	10
srcserver	Source server	uint8	3
srcssid	Source SSID	string	33
srcswversion		string	66
srcuuid	UUID of the Source Address Object	string	37
sslaction	Action taken by ssl-ssh-profile	string	26
subtype	Subtype of the traffic	string	20
time	Time	string	8
trandisp	NAT translation type	string	16
tranip	NAT Destination IP	ip	39
tranport	NAT Destination Port	uint16	5
transip	NAT Source IP	ip	39
transport	NAT Source Protocol Port	uint16	5
tunnelid		uint32	10
type	Log type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user name	string	66
unauthusersource	The method used to detect unauthenticated user name	string	66
url	URL	string	512
user	User name	string	256
utmaction	Security action performed by UTM	string	32
vd	Virtual domain name	string	32
vpn	The name of the VPN tunnel	string	32
vpntype	The type of the VPN tunnel	string	14
vrf	Virtual router forwarding	uint8	3
vwlid	Virtual Wan Link (SD-WAN) service id	uint32	10
vwlname		string	36

Log Field Name	Description	Data Type	Length
vwlquality	Quality info of the service rule that is matched by traffic	string	320
vwlservice	Application that is matched by the traffic (internet-service-app-ctrl)	string	64
vwpvlanid	Virtual Wire Pair vlan id	uint32	10
wanin	WAN incoming traffic in bytes	uint64	20
wanoptapptype	WAN Optimization Application type	string	9
wanout	WAN outgoing traffic in bytes	uint64	20
countapp	Number of App Ctrl logs associated with the session	uint32	10
countav	Number of AV logs associated with the session	uint32	10
countcifs		uint32	10
countdlp	Number of DLP logs associated with the session	uint32	10
countdns	Number of DNS Query logs associated with the session	uint32	10
countemail	Number of Email logs associated with the session	uint32	10
countff		uint32	10
counticap		uint32	10
countips	Number of IPS logs associated with the session	uint32	10
countssh	Number of SSH logs associated with the session	uint32	10
countssl		uint32	10
countwaf	Number of WAF logs associated with the session	uint32	10
countweb	Number of Web Filter logs associated with the session	uint32	10

## VoIP

### 44032 - LOGID\_EVENT\_VOIP\_SIP

**Message ID:** 44032

**Message Description:** LOGID\_EVENT\_VOIP\_SIP

**Message Meaning:** VoIP SIP

**Type:** VoIP

**Category:** VOIP

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Day, month, and year when the log message was recorded.	string	10
time	Hour clock when the log message was recorded.	string	8
logid	Unique Log ID	string	10
type	Type of log. Ex: type="utm"	string	16
subtype	Subtype	string	20
level	Log Level	string	11
devid	Serial number of the device for the traffic's origin.	string	16
vd	Name of the virtual domain in which the log message was recorded.	string	32
eventtime	Time when event occurred	uint64	20
tz	Time zone	string	5
session_id	Session ID. Ex: session_id=232	uint32	10
epoch	Epoch	uint32	10
event_id	Unique event ID	uint32	10
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
dstip	Destination IP	ip	39
dst_port	Destination port	uint16	5
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
src_int	Name of the source interface. Ex: src_int="port1"	string	16
dst_int	Destination Interface	string	16
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
profile	Name or number of associated VOIP profile	string	64
voip_proto	SIP/SCCP/MGCP/h323	string	4
kind	Kind of service. Typically it will have value "call"	string	10
action	Action. Eg. block , allow	string	15
status	Status. Ex: status="blocked" , status= "start"	string	23
duration	Duration of the session. Ex: 180 (in seconds)	uint32	10
dir	Destination Interface	string	16

Log Field Name	Description	Data Type	Length
call_id	Ex: call_id="1-22011@10.6.30.11"	string	64
from	Where call was originated from	string	128
to	Destination address	string	512

## 44033 - LOGID\_EVENT\_VOIP\_SIP\_BLOCK

**Message ID:** 44033

**Message Description:** LOGID\_EVENT\_VOIP\_SIP\_BLOCK

**Message Meaning:** VoIP SIP blocked

**Type:** VoIP

**Category:** VOIP

**Severity:** Notice

Log Field Name	Description	Data Type	Length
date	Day, month, and year when the log message was recorded.	string	10
time	Hour clock when the log message was recorded.	string	8
logid	Unique Log ID	string	10
type	Type of log. Ex: type="utm"	string	16
subtype	Subtype	string	20
level	Log Level	string	11
devid	Serial number of the device for the traffic's origin.	string	16
vd	Name of the virtual domain in which the log message was recorded.	string	32
eventtime	Time when event occurred	uint64	20
tz	Time zone	string	5
session_id	Session ID. Ex: session_id=232	uint32	10
epoch	Epoch	uint32	10
event_id	Unique event ID	uint32	10
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
dstip	Destination IP	ip	39
dst_port	Destination port	uint16	5

Log Field Name	Description	Data Type	Length
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
src_int	Name of the source interface. Ex: src_int="port1"	string	16
dst_int	Destination Interface	string	16
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
profile	Name or number of associated VOIP profile	string	64
voip_proto	SIP/SCCP/MGCP/h323	string	4
kind	Kind of service. Typically it will have value "call"	string	10
action	Action. Eg. block , allow	string	15
status	Status. Ex: status="blocked" , status= "start"	string	23
duration	Duration of the session. Ex: 180 (in seconds)	uint32	10
dir	Destination Interface	string	16
call_id	Ex: call_id="1-22011@10.6.30.11"	string	64
from	Where call was originated from	string	128
to	Destination address	string	512
reason	Reason. Ex: reason="unrecognized-form"	string	128
message_type	Message Type. Ex: message_type="request"	string	16
request_name	Name of request. Ex: request_name="INVITE" or "NOTIFY"	string	64
count	Session count	uint32	10

## 44034 - LOGID\_EVENT\_VOIP\_SIP\_FUZZING

**Message ID:** 44034

**Message Description:** LOGID\_EVENT\_VOIP\_SIP\_FUZZING

**Message Meaning:** VoIP SIP fuzzing

**Type:** VoIP

**Category:** VOIP

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Day, month, and year when the log message was recorded.	string	10
time	Hour clock when the log message was recorded.	string	8
logid	Unique Log ID	string	10



Log Field Name	Description	Data Type	Length
type	Type of log. Ex: type="utm"	string	16
subtype	Subtype	string	20
level	Log Level	string	11
devid	Serial number of the device for the traffic's origin.	string	16
vd	Name of the virtual domain in which the log message was recorded.	string	32
eventtime	Time when event occurred	uint64	20
tz	Time zone	string	5
session_id	Session ID. Ex: session_id=232	uint32	10
epoch	Epoch	uint32	10
event_id	Unique event ID	uint32	10
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
dstip	Destination IP	ip	39
dst_port	Destination port	uint16	5
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
src_int	Name of the source interface. Ex: src_int="port1"	string	16
dst_int	Destination Interface	string	16
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
profile	Name or number of associated VOIP profile	string	64
voip_proto	SIP/SCCP/MGCP/h323	string	4
kind	Kind of service. Typically it will have value "call"	string	10
action	Action. Eg. block , allow	string	15
duration	Duration of the session. Ex: 180 (in seconds)	uint32	10
dir	Destination Interface	string	16
call_id	Ex: call_id="1-22011@10.6.30.11"	string	64
message_type	Message Type. Ex: message_type="request"	string	16
request_name	Name of request. Ex: request_name="INVITE" or "NOTIFY"	string	64
malform_desc	Malformed header description	string	47

Log Field Name	Description	Data Type	Length
malform_data	Malformed header data	uint32	10
line	SIP header line	string	128
column	Ex: column=16	uint32	10

## 44035 - LOGID\_EVENT\_VOIP\_SCCP\_REGISTER

**Message ID:** 44035

**Message Description:** LOGID\_EVENT\_VOIP\_SCCP\_REGISTER

**Message Meaning:** VoIP SCCP registered

**Type:** VoIP

**Category:** VOIP

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Day, month, and year when the log message was recorded.	string	10
time	Hour clock when the log message was recorded.	string	8
logid	Unique Log ID	string	10
type	Type of log. Ex: type="utm"	string	16
subtype	Subtype	string	20
level	Log Level	string	11
devid	Serial number of the device for the traffic's origin.	string	16
vd	Name of the virtual domain in which the log message was recorded.	string	32
eventtime	Time when event occurred	uint64	20
tz	Time zone	string	5
session_id	Session ID. Ex: session_id=232	uint32	10
epoch	Epoch	uint32	10
event_id	Unique event ID	uint32	10
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
dstip	Destination IP	ip	39
dst_port	Destination port	uint16	5

Log Field Name	Description	Data Type	Length
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
src_int	Name of the source interface. Ex: src_int="port1"	string	16
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
profile	Name or number of associated VOIP profile	string	64
voip_proto	SIP/SCCP/MGCP/h323	string	4
kind	Kind of service. Typically it will have value "call"	string	10
action	Action. Eg. block , allow	string	15
status	Status. Ex: status="blocked" , status= "start"	string	23
locip	Local IP	ip	39
phone	Phone	string	64

## 44036 - LOGID\_EVENT\_VOIP\_SCCP\_UNREGISTER

**Message ID:** 44036

**Message Description:** LOGID\_EVENT\_VOIP\_SCCP\_UNREGISTER

**Message Meaning:** VoIP SCCP unregistered

**Type:** VoIP

**Category:** VOIP

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Day, month, and year when the log message was recorded.	string	10
time	Hour clock when the log message was recorded.	string	8
logid	Unique Log ID	string	10
type	Type of log. Ex: type="utm"	string	16
subtype	Subtype	string	20
level	Log Level	string	11
devid	Serial number of the device for the traffic's origin.	string	16
vd	Name of the virtual domain in which the log message was recorded.	string	32
eventtime	Time when event occurred	uint64	20

Log Field Name	Description	Data Type	Length
tz	Time zone	string	5
session_id	Session ID. Ex: session_id=232	uint32	10
epoch	Epoch	uint32	10
event_id	Unique event ID	uint32	10
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
dstip	Destination IP	ip	39
dst_port	Destination port	uint16	5
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
src_int	Name of the source interface. Ex: src_int="port1"	string	16
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
profile	Name or number of associated VOIP profile	string	64
voip_proto	SIP/SCCP/MGCP/h323	string	4
kind	Kind of service. Typically it will have value "call"	string	10
action	Action. Eg. block , allow	string	15
status	Status. Ex: status="blocked" , status= "start"	string	23
reason	Reason. Ex: reason="unrecognized-form"	string	128
locip	Local IP	ip	39
phone	Phone	string	64

## 44037 - LOGID\_EVENT\_VOIP\_SCCP\_CALL\_BLOCK

**Message ID:** 44037

**Message Description:** LOGID\_EVENT\_VOIP\_SCCP\_CALL\_BLOCK

**Message Meaning:** VoIP SCCP call blocked

**Type:** VoIP

**Category:** VOIP

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Day, month, and year when the log message was recorded.	string	10
time	Hour clock when the log message was recorded.	string	8

Log Field Name	Description	Data Type	Length
logid	Unique Log ID	string	10
type	Type of log. Ex: type="utm"	string	16
subtype	Subtype	string	20
level	Log Level	string	11
devid	Serial number of the device for the traffic's origin.	string	16
vd	Name of the virtual domain in which the log message was recorded.	string	32
eventtime	Time when event occurred	uint64	20
tz	Time zone	string	5
session_id	Session ID. Ex: session_id=232	uint32	10
epoch	Epoch	uint32	10
event_id	Unique event ID	uint32	10
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
dstip	Destination IP	ip	39
dst_port	Destination port	uint16	5
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
src_int	Name of the source interface. Ex: src_int="port1"	string	16
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
profile	Name or number of associated VOIP profile	string	64
voip_proto	SIP/SCCP/MGCP/h323	string	4
kind	Kind of service. Typically it will have value "call"	string	10
action	Action. Eg. block , allow	string	15
status	Status. Ex: status="blocked" , status="start"	string	23
reason	Reason. Ex: reason="unrecognized-form"	string	128
locip	Local IP	ip	39
phone	Phone	string	64

## 44038 - LOGID\_EVENT\_VOIP\_SCCP\_CALL\_INFO

**Message ID:** 44038

**Message Description:** LOGID\_EVENT\_VOIP\_SCCP\_CALL\_INFO

**Message Meaning:** VoIP SCCP call information

**Type:** VoIP

**Category:** VOIP

**Severity:** Information

Log Field Name	Description	Data Type	Length
date	Day, month, and year when the log message was recorded.	string	10
time	Hour clock when the log message was recorded.	string	8
logid	Unique Log ID	string	10
type	Type of log. Ex: type="utm"	string	16
subtype	Subtype	string	20
level	Log Level	string	11
devid	Serial number of the device for the traffic's origin.	string	16
vd	Name of the virtual domain in which the log message was recorded.	string	32
eventtime	Time when event occurred	uint64	20
tz	Time zone	string	5
session_id	Session ID. Ex: session_id=232	uint32	10
epoch	Epoch	uint32	10
event_id	Unique event ID	uint32	10
srcip	IP address of the traffic's origin. Ex: srcip=10.1.100.155	ip	39
src_port	Port number of the traffic's origin. Ex: srcport=40772	uint16	5
dstip	Destination IP	ip	39
dst_port	Destination port	uint16	5
proto	Protocol number. Ex: for SIP it will be proto=17	uint8	3
src_int	Name of the source interface. Ex: src_int="port1"	string	16
dst_int	Destination Interface	string	16
policy_id	Name of the firewall policy governing the traffic which caused the log message.	uint32	10
profile	Name or number of associated VOIP profile	string	64
voip_proto	SIP/SCCP/MGCP/h323	string	4
kind	Kind of service. Typically it will have value "call"	string	10

Log Field Name	Description	Data Type	Length
action	Action. Eg. block , allow	string	15
status	Status. Ex: status="blocked" , status= "start"	string	23
duration	Duration of the session. Ex: 180 (in seconds)	uint32	10
locip	Local IP	ip	39
phone	Phone	string	64
locport	Local Port	uint16	5
remip	Remote IP	ip	39
remport	Remote Port	uint16	5

## WAF

### 30248 - LOGID\_WAF\_SIGNATURE\_BLOCK

**Message ID:** 30248

**Message Description:** LOGID\_WAF\_SIGNATURE\_BLOCK

**Message Meaning:** Web application firewall blocked application by signature

**Type:** WAF

**Category:** WAF-SIGNATURE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32

Log Field Name	Description	Data Type	Length
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66



Log Field Name	Description	Data Type	Length
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## 30249 - LOGID\_WAF\_SIGNATURE\_PASS

**Message ID:** 30249

**Message Description:** LOGID\_WAF\_SIGNATURE\_PASS

**Message Meaning:** Web application firewall passed application by signature

**Type:** WAF

**Category:** WAF-SIGNATURE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32

Log Field Name	Description	Data Type	Length
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## 30250 - LOGID\_WAF\_SIGNATURE\_ERASE

**Message ID:** 30250

**Message Description:** LOGID\_WAF\_SIGNATURE\_ERASE

**Message Meaning:** Web application firewall erased application by signature

**Type:** WAF

**Category:** WAF-SIGNATURE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3

Log Field Name	Description	Data Type	Length
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## 30251 - LOGID\_WAF\_CUSTOM\_SIGNATURE\_BLOCK

**Message ID:** 30251

**Message Description:** LOGID\_WAF\_CUSTOM\_SIGNATURE\_BLOCK

**Message Meaning:** Web application firewall blocked application by custom signature

**Type:** WAF

**Category:** WAF-CUSTOM-SIGNATURE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

Log Field Name	Description	Data Type	Length
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10

Log Field Name	Description	Data Type	Length
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## 30252 - LOGID\_WAF\_CUSTOM\_SIGNATURE\_PASS

**Message ID:** 30252

**Message Description:** LOGID\_WAF\_CUSTOM\_SIGNATURE\_PASS

**Message Meaning:** Web application firewall allowed application by custom signature

**Type:** WAF

**Category:** WAF-CUSTOM-SIGNATURE

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32

Log Field Name	Description	Data Type	Length
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66

Log Field Name	Description	Data Type	Length
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## 30253 - LOGID\_WAF\_METHOD\_BLOCK

**Message ID:** 30253

**Message Description:** LOGID\_WAF\_METHOD\_BLOCK

**Message Meaning:** Web application firewall blocked application by HTTP method

**Type:** WAF

**Category:** WAF-HTTP-METHOD

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32



Log Field Name	Description	Data Type	Length
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## 30255 - LOGID\_WAF\_ADDRESS\_LIST\_BLOCK

**Message ID:** 30255

**Message Description:** LOGID\_WAF\_ADDRESS\_LIST\_BLOCK

**Message Meaning:** Web application firewall blocked application by address list

**Type:** WAF

**Category:** WAF-ADDRESS-LIST

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3

Log Field Name	Description	Data Type	Length
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## 30257 - LOGID\_WAF\_CONSTRAINTS\_BLOCK

**Message ID:** 30257

**Message Description:** LOGID\_WAF\_CONSTRAINTS\_BLOCK

**Message Meaning:** Web application firewall blocked application by HTTP constraints

**Type:** WAF

**Category:** WAF-HTTP-CONSTRAINT

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

Log Field Name	Description	Data Type	Length
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10

Log Field Name	Description	Data Type	Length
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## 30258 - LOGID\_WAF\_CONSTRAINTS\_PASS

**Message ID:** 30258

**Message Description:** LOGID\_WAF\_CONSTRAINTS\_PASS

**Message Meaning:** Web application firewall allowed application by HTTP constraints

**Type:** WAF

**Category:** WAF-HTTP-CONSTRAINT

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32

Log Field Name	Description	Data Type	Length
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66

Log Field Name	Description	Data Type	Length
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## 30259 - LOGID\_WAF\_URL\_ACCESS\_PERMIT

**Message ID:** 30259

**Message Description:** LOGID\_WAF\_URL\_ACCESS\_PERMIT

**Message Meaning:** Web application firewall allowed application by URL access permit

**Type:** WAF

**Category:** WAF-URL-ACCESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32

Log Field Name	Description	Data Type	Length
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## 30260 - LOGID\_WAF\_URL\_ACCESS\_BYPASS

**Message ID:** 30260

**Message Description:** LOGID\_WAF\_URL\_ACCESS\_BYPASS



**Message Meaning:** Web application firewall allowed application by URL access bypass

**Type:** WAF

**Category:** WAF-URL-ACCESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3

Log Field Name	Description	Data Type	Length
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## 30261 - LOGID\_WAF\_URL\_ACCESS\_BLOCK

**Message ID:** 30261

**Message Description:** LOGID\_WAF\_URL\_ACCESS\_BLOCK

**Message Meaning:** Web application firewall blocked application by URL access

**Type:** WAF

**Category:** WAF-URL-ACCESS

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Status of the session. Uses following definition: - Deny = blocked by firewall policy. - Start = session start log (special option to enable logging at start of a session). This means firewall allowed. - All Others = allowed by Firewall Policy and the status indicates how it was closed.	string	17

Log Field Name	Description	Data Type	Length
agent	Agent	string	64
authserver	Authentication Server	string	64
constraint	WAF HTTP protocol restrictions	string	4096
date	Date	string	10
devid	Device ID	string	16
direction	Direction	string	4096
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP Address	ip	39
dstport	Destination Port	uint16	5
eventid	Event ID	uint32	10
eventtime	Event Time, Time when WAF event detected	uint64	20
eventtype	Event Type	string	32
fctuid	FortiClient UID	string	32
group	User Group Name	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	HTTP Method	string	4096
msg	Log Message	string	4096
name	Method or custom signature name	string	64
policyid	Policy ID	uint32	10
profile	Full profile name	string	64
proto	Protocol	uint8	3
rawdata	Raw Data	string	1024
service	Service name	string	5
sessionid	Session ID	uint32	10
severity	Severity	string	6
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10

Log Field Name	Description	Data Type	Length
srcip	Source IP Address	ip	39
srcport	Source Port	uint16	5
subtype	Log Subtype	string	20
time	Time	string	8
type	Log Type	string	16
tz	Time zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	URL	string	512
user	User Name	string	256
vd	Virtual Domain Name	string	32

## Web

### 12288 - LOG\_ID\_WEB\_CONTENT\_BANWORD

**Message ID:** 12288

**Message Description:** LOG\_ID\_WEB\_CONTENT\_BANWORD

**Message Meaning:** Web content banned word found

**Type:** Web

**Category:** CONTENT

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Authentication server for the user	string	64
banword	Banned word	string	128
contenttype	Content Type from HTTP header	string	64
craction	Client Reputation Action	uint32	10

Log Field Name	Description	Data Type	Length
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
from	MMS-only - From/To headers from the email	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
keyword	Keyword used for search	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20

Log Field Name	Description	Data Type	Length
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
to	MMS-only - From/To headers from the email	string	512
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12290 - LOG\_ID\_WEB\_CONTENT\_EXEMPTWORD

**Message ID:** 12290

**Message Description:** LOG\_ID\_WEB\_CONTENT\_EXEMPTWORD

**Message Meaning:** Web content exempt word found

**Type:** Web

**Category:** CONTENT

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Authentication server for the user	string	64
banword	Banned word	string	128
contenttype	Content Type from HTTP header	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
from	MMS-only - From/To headers from the email	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
keyword	Keyword used for search	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3

Log Field Name	Description	Data Type	Length
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
to	MMS-only - From/To headers from the email	string	512
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12292 - LOG\_ID\_WEB\_CONTENT\_KEYWORD

**Message ID:** 12292

**Message Description:** LOG\_ID\_WEB\_CONTENT\_KEYWORD

**Message Meaning:** Message contained a key word in the profile list

**Type:** Web



**Category:** CONTENT**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Authentication server for the user	string	64
banword	Banned word	string	128
contenttype	Content Type from HTTP header	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
from	MMS-only - From/To headers from the email	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
keyword	Keyword used for search	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referrallurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
to	MMS-only - From/To headers from the email	string	512
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12293 - LOG\_ID\_WEB\_CONTENT\_SEARCH

**Message ID:** 12293

**Message Description:** LOG\_ID\_WEB\_CONTENT\_SEARCH**Message Meaning:** Search phrase detected**Type:** Web**Category:** CONTENT**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Authentication server for the user	string	64
banword	Banned word	string	128
contenttype	Content Type from HTTP header	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
from	MMS-only - From/To headers from the email	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
keyword	Keyword used for search	string	512
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
to	MMS-only - From/To headers from the email	string	512
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12544 - LOG\_ID\_URL\_FILTER\_BLOCK

**Message ID:** 12544

**Message Description:** LOG\_ID\_URL\_FILTER\_BLOCK

**Message Meaning:** URL address was blocked because it was found in the URL filter list

**Type:** Web

**Category:** URLFILTER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referrallurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
urlfilteridx	URL filter ID	uint32	10
urlfilterlist	URL filter list	string	64
urlsource	URL source	string	64
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12545 - LOG\_ID\_URL\_FILTER\_EXEMPT

**Message ID:** 12545

**Message Description:** LOG\_ID\_URL\_FILTER\_EXEMPT

**Message Meaning:** URL address was exempted because it was found in the URL filter list

**Type:** Web

**Category:** URLFILTER

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referrallurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
urlfilteridx	URL filter ID	uint32	10
urlfilterlist	URL filter list	string	64
urlsource	URL source	string	64
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3



## 12546 - LOG\_ID\_URL\_FILTER\_ALLOW

**Message ID:** 12546

**Message Description:** LOG\_ID\_URL\_FILTER\_ALLOW

**Message Meaning:** URL address was allowed because it was found in the URL filter list

**Type:** Web

**Category:** URLFILTER

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referrallurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
urlfilteridx	URL filter ID	uint32	10
urlfilterlist	URL filter list	string	64
urlsource	URL source	string	64
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12547 - LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_HTTP\_BLK

**Message ID:** 12547

**Message Description:** LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_HTTP\_BLK

**Message Meaning:** The request contained an invalid domain name

**Type:** Web

**Category:** URLFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10

Log Field Name	Description	Data Type	Length
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12548 - LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_HTTPS\_BLK

**Message ID:** 12548

**Message Description:** LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_HTTPS\_BLK

**Message Meaning:** HTTP certificate request contained an invalid domain name

**Type:** Web

**Category:** URLFILTER**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referrurl	Referrer URI	string	512

Log Field Name	Description	Data Type	Length
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12549 - LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_HTTP\_PASS

**Message ID:** 12549

**Message Description:** LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_HTTP\_PASS

**Message Meaning:** HTTP request contained an invalid name so the session has been filtered by IP only

**Type:** Web

**Category:** URLFILTER

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20

Log Field Name	Description	Data Type	Length
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12550 - LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_HTTPS\_PASS

**Message ID:** 12550

**Message Description:** LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_HTTPS\_PASS

**Message Meaning:** HTTPS request contained an invalid name so the session has been filtered by IP only

**Type:** Web

**Category:** URLFILTER

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64



Log Field Name	Description	Data Type	Length
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12551 - LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_SNI\_BLK

**Message ID:** 12551

**Message Description:** LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_SNI\_BLK

**Message Meaning:** Insufficient resources

**Type:** Web

**Category:** URLFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10

Log Field Name	Description	Data Type	Length
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12552 - LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_SNI\_PASS

**Message ID:** 12552

**Message Description:** LOG\_ID\_URL\_FILTER\_INVALID\_HOSTNAME\_SNI\_PASS

**Message Meaning:** Getting the host name failed

**Type:** Web

**Category:** URLFILTER

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8

Log Field Name	Description	Data Type	Length
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8

Log Field Name	Description	Data Type	Length
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12553 - LOG\_ID\_URL\_FILTER\_INVALID\_CERT

**Message ID:** 12553

**Message Description:** LOG\_ID\_URL\_FILTER\_INVALID\_CERT

**Message Meaning:** Server certificate validation failed

**Type:** Web

**Category:** URLFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39

Log Field Name	Description	Data Type	Length
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5

Log Field Name	Description	Data Type	Length
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12554 - LOG\_ID\_URL\_FILTER\_INVALID\_SESSION

**Message ID:** 12554

**Message Description:** LOG\_ID\_URL\_FILTER\_INVALID\_SESSION

**Message Meaning:** SSL session blocked because its identification number was unknown

**Type:** Web

**Category:** URLFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32



Log Field Name	Description	Data Type	Length
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512

Log Field Name	Description	Data Type	Length
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12555 - LOG\_ID\_URL\_FILTER\_SRV\_CERT\_ERR\_BLK

**Message ID:** 12555

**Message Description:** LOG\_ID\_URL\_FILTER\_SRV\_CERT\_ERR\_BLK

**Message Meaning:** SSL session blocked

**Type:** Web

**Category:** URLFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64

Log Field Name	Description	Data Type	Length
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referrurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

**12556 - LOG\_ID\_URL\_FILTER\_SRV\_CERT\_ERR\_PASS****Message ID:** 12556**Message Description:** LOG\_ID\_URL\_FILTER\_SRV\_CERT\_ERR\_PASS**Message Meaning:** SSL session ignored**Type:** Web**Category:** URLFILTER**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10

Log Field Name	Description	Data Type	Length
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12557 - LOG\_ID\_URL\_FILTER\_FAMS\_NOT\_ACTIVE

**Message ID:** 12557

**Message Description:** LOG\_ID\_URL\_FILTER\_FAMS\_NOT\_ACTIVE

**Message Meaning:** The FortiGuard Analysis and Management Service is not active. You must enable this service

**Type:** Web

**Category:** URLFILTER**Severity:** Critical

Log Field Name	Description	Data Type	Length
date	Date	string	10
devid	Device ID	string	16
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz	Time Zone	string	5
vd	Virtual domain name	string	32

## 12558 - LOG\_ID\_URL\_FILTER\_RATING\_ERR

**Message ID:** 12558**Message Description:** LOG\_ID\_URL\_FILTER\_RATING\_ERR**Message Meaning:** Rating error occurred**Type:** Web**Category:** URLFILTER**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16

Log Field Name	Description	Data Type	Length
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
srcdomain		string	255
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
error	URL rating error message	string	256
urltype	URL filter type	string	8

## 12559 - LOG\_ID\_URL\_FILTER\_PASS

**Message ID:** 12559

**Message Description:** LOG\_ID\_URL\_FILTER\_PASS

**Message Meaning:** URL passed because it was in the URL filter list

**Type:** Web

**Category:** URLFILTER

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512



Log Field Name	Description	Data Type	Length
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
urlfilteridx	URL filter ID	uint32	10
urlfilterlist	URL filter list	string	64
urlsource	URL source	string	64
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12560 - LOG\_ID\_URL\_WISP\_BLOCK

**Message ID:** 12560

**Message Description:** LOG\_ID\_URL\_WISP\_BLOCK

**Message Meaning:** URL blocked by Websense service

**Type:** Web

**Category:** URLFILTER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20

Log Field Name	Description	Data Type	Length
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12561 - LOG\_ID\_URL\_WISP\_REDIR

**Message ID:** 12561

**Message Description:** LOG\_ID\_URL\_WISP\_REDIR

**Message Meaning:** URL blocked with redirect message by Websense service

**Type:** Web

**Category:** URLFILTER

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64

Log Field Name	Description	Data Type	Length
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255

Log Field Name	Description	Data Type	Length
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12562 - LOG\_ID\_URL\_WISP\_ALLOW

**Message ID:** 12562

**Message Description:** LOG\_ID\_URL\_WISP\_ALLOW

**Message Meaning:** URL allowed by Websense service

**Type:** Web

**Category:** URLFILTER

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10

Log Field Name	Description	Data Type	Length
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12688 - LOG\_ID\_WEB\_SSL\_EXEMPT

**Message ID:** 12688

**Message Description:** LOG\_ID\_WEB\_SSL\_EXEMPT

**Message Meaning:** URL address was exempted because it was found in the ssl-exempt

**Type:** Web

**Category:** SSL-EXEMPT

**Severity:** Information

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20



Log Field Name	Description	Data Type	Length
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
urlsource	URL source	string	64
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12800 - LOG\_ID\_WEB\_FTGD\_ERR

**Message ID:** 12800

**Message Description:** LOG\_ID\_WEB\_FTGD\_ERR

**Message Meaning:** Rating error occurred (error)

**Type:** Web

**Category:** FTGD\_ERR

**Severity:** Error

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	URL rating error message	string	256
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8

Log Field Name	Description	Data Type	Length
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12801 - LOG\_ID\_WEB\_FTGD\_WARNING

**Message ID:** 12801

**Message Description:** LOG\_ID\_WEB\_FTGD\_WARNING

**Message Meaning:** Rating error occurred (warning)

**Type:** Web

**Category:** FTGD\_ERR

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
error	URL rating error message	string	256
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8

Log Field Name	Description	Data Type	Length
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 12802 - LOG\_ID\_WEB\_FTGD\_QUOTA

**Message ID:** 12802

**Message Description:** LOG\_ID\_WEB\_FTGD\_QUOTA

**Message Meaning:** Daily FortiGuard quota status

**Type:** Web

**Category:** FTGD\_QUOTA

**Severity:** Information

Log Field Name	Description	Data Type	Length
catdesc	Web category description	string	64
date	Date	string	10

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
level	Log Level	string	11
logid	Log ID	string	10
profile	Web Filter profile name	string	64
quotaexceeded	Quota has been exceeded	string	3
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
subtype	Log subtype	string	20
time	Time	string	8
type	Log type	string	16
tz	Time Zone	string	5
user	User name	string	256
vd	Virtual domain name	string	32

## 13056 - LOG\_ID\_WEB\_FTGD\_CAT\_BLK

**Message ID:** 13056

**Message Description:** LOG\_ID\_WEB\_FTGD\_CAT\_BLK

**Message Meaning:** URL belongs to an blocked category within the firewall policy

**Type:** Web

**Category:** FTGD\_BLK

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
cat	Web category ID	uint8	3

Log Field Name	Description	Data Type	Length
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20

Log Field Name	Description	Data Type	Length
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
urlsource	URL source	string	64
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13057 - LOG\_ID\_WEB\_FTGD\_CAT\_WARN

**Message ID:** 13057

**Message Description:** LOG\_ID\_WEB\_FTGD\_CAT\_WARN

**Message Meaning:** URL belongs to a category with warnings enabled

**Type:** Web



**Category:** FTGD\_BLK**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64

Log Field Name	Description	Data Type	Length
proto	Protocol number	uint8	3
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
urlsource	URL source	string	64
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13312 - LOG\_ID\_WEB\_FTGD\_CAT\_ALLOW

**Message ID:** 13312

**Message Description:** LOG\_ID\_WEB\_FTGD\_CAT\_ALLOW

**Message Meaning:** URL belongs to an allowed category within the firewall policy

**Type:** Web

**Category:** FTGD\_ALLOW

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11

Log Field Name	Description	Data Type	Length
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66

Log Field Name	Description	Data Type	Length
url	The URL address	string	512
urlsource	URL source	string	64
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13315 - LOG\_ID\_WEB\_FTGD\_QUOTA\_COUNTING

**Message ID:** 13315

**Message Description:** LOG\_ID\_WEB\_FTGD\_QUOTA\_COUNTING

**Message Meaning:** FortiGuard web filter category quota counting log message

**Type:** Web

**Category:** FTGD\_QUOTA\_COUNTING

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20

Log Field Name	Description	Data Type	Length
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5

Log Field Name	Description	Data Type	Length
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
urlsource	URL source	string	64
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13317 - LOG\_ID\_WEB\_URL

**Message ID:** 13317

**Message Description:** LOG\_ID\_WEB\_URL

**Message Meaning:** URL has been visited

**Type:** Web

**Category:** URLMONITOR

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
authserver	Authentication server for the user	string	64
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10

Log Field Name	Description	Data Type	Length
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
quotamax	Maximum quota allowed - in seconds if time-based - in bytes if traffic-based	uint64	20
quotatype	Quota type	string	16
quotaused	Quota used - in seconds if time-based - in bytes if traffic-based	uint64	20
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20



Log Field Name	Description	Data Type	Length
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
urlsource	URL source	string	64
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13568 - LOG\_ID\_WEB\_SCRIPTFILTER\_ACTIVEX

**Message ID:** 13568

**Message Description:** LOG\_ID\_WEB\_SCRIPTFILTER\_ACTIVEX

**Message Meaning:** ActiveX script removed

**Type:** Web

**Category:** ACTIVEXFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
filtertype	Filter type	string	10
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8

Log Field Name	Description	Data Type	Length
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13573 - LOG\_ID\_WEB\_SCRIPTFILTER\_COOKIE

**Message ID:** 13573

**Message Description:** LOG\_ID\_WEB\_SCRIPTFILTER\_COOKIE

**Message Meaning:** Cookie removed

**Type:** Web

**Category:** COOKIEFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
filtertype	Filter type	string	10
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8

Log Field Name	Description	Data Type	Length
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13584 - LOG\_ID\_WEB\_SCRIPTFILTER\_APPLET

**Message ID:** 13584

**Message Description:** LOG\_ID\_WEB\_SCRIPTFILTER\_APPLET

**Message Meaning:** Java applet removed

**Type:** Web

**Category:** APPLETFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
filtertype	Filter type	string	10
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8

Log Field Name	Description	Data Type	Length
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13600 - LOG\_ID\_WEB\_SCRIPTFILTER\_OTHER

**Message ID:** 13600

**Message Description:** LOG\_ID\_WEB\_SCRIPTFILTER\_OTHER

**Message Meaning:** Script entity removed

**Type:** Web

**Category:** SCRIPTFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
filtertype	Filter type	string	10
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8



Log Field Name	Description	Data Type	Length
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13601 - LOG\_ID\_WEB\_WF\_COOKIE

**Message ID:** 13601

**Message Description:** LOG\_ID\_WEB\_WF\_COOKIE

**Message Meaning:** Cookie removed entirely

**Type:** Web

**Category:** COOKIEFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
filtertype	Filter type	string	10
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8

Log Field Name	Description	Data Type	Length
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13602 - LOG\_ID\_WEB\_WF\_REFERER

**Message ID:** 13602

**Message Description:** LOG\_ID\_WEB\_WF\_REFERER

**Message Meaning:** Referrer removed from request

**Type:** Web

**Category:** COOKIEFILTER

**Severity:** Notice

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
filtertype	Filter type	string	10
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8

Log Field Name	Description	Data Type	Length
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13603 - LOG\_ID\_WEB\_WF\_COMMAND\_BLOCK

**Message ID:** 13603

**Message Description:** LOG\_ID\_WEB\_WF\_COMMAND\_BLOCK

**Message Meaning:** Command blocked

**Type:** Web

**Category:** WEBFILTER\_COMMAND\_BLOCK

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11

Log Field Name	Description	Data Type	Length
authserver	Authentication server for the user	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referrallurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13616 - LOG\_ID\_CONTENT\_TYPE\_BLOCK

**Message ID:** 13616

**Message Description:** LOG\_ID\_CONTENT\_TYPE\_BLOCK

**Message Meaning:** Blocked by HTTP header content type

**Type:** Web

**Category:** CONTENT

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Authentication server for the user	string	64
banword	Banned word	string	128

Log Field Name	Description	Data Type	Length
contenttype	Content Type from HTTP header	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
from	MMS-only - From/To headers from the email	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
keyword	Keyword used for search	string	512
level	Log Level	string	11
logid	Log ID	string	10
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512



Log Field Name	Description	Data Type	Length
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
to	MMS-only - From/To headers from the email	string	512
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13632 - LOGID\_HTTP\_HDR\_CHG\_REQ

**Message ID:** 13632

**Message Description:** LOGID\_HTTP\_HDR\_CHG\_REQ

**Message Meaning:** Depends on info in msg field

**Type:** Web

**Category:** HTTP\_HEADER\_CHANGE

**Severity:** Notice

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Authentication server for the user	string	64
chgheaders	Change headers	string	1024
date	Date	string	10
devid	Device ID	string	16
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
group	User group name	string	64
level	Log Level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
service	Service name	string	36
sessionid	Session ID	uint32	10
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
transid	Transaction ID	uint32	10
type	Log type	string	16
tz	Time Zone	string	5
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32

## 13633 - LOGID\_HTTP\_HDR\_CHG\_RESP

**Message ID:** 13633

**Message Description:** LOGID\_HTTP\_HDR\_CHG\_RESP

**Message Meaning:** Depends on info in msg field

**Type:** Web

**Category:** HTTP\_HEADER\_CHANGE

**Severity:** Notice

Log Field Name	Description	Data Type	Length
agent	User agent - eg. agent="Mozilla/5.0"	string	64
authserver	Authentication server for the user	string	64
chgheaders	Change headers	string	1024
date	Date	string	10
devid	Device ID	string	16
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
group	User group name	string	64
level	Log Level	string	11
logid	Log ID	string	10
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
service	Service name	string	36
sessionid	Session ID	uint32	10
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5

Log Field Name	Description	Data Type	Length
subtype	Log subtype	string	20
time	Time	string	8
transid	Transaction ID	uint32	10
type	Log type	string	16
tz	Time Zone	string	5
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32

## 13648 - LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_URL\_ALLOW

**Message ID:** 13648

**Message Description:** LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_URL\_ALLOW

**Message Meaning:** Antiphishing matched a URL filter rule without blocking the request.

**Type:** Web

**Category:** ANTIPHISHING

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
antiphishdc		string	64
antiphishrule		string	64
authserver	Authentication server for the user	string	64
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8

Log Field Name	Description	Data Type	Length
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39

Log Field Name	Description	Data Type	Length
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13649 - LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_FTGD\_ALLOW

**Message ID:** 13649

**Message Description:** LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_FTGD\_ALLOW

**Message Meaning:** Antiphishing matched a Fortiguard category rule without blocking the request.

**Type:** Web

**Category:** ANTIPHISHING

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
antiphishdc		string	64
antiphishrule		string	64
authserver	Authentication server for the user	string	64
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10

Log Field Name	Description	Data Type	Length
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referrallurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10

Log Field Name	Description	Data Type	Length
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13650 - LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_DEFAULT\_ALLOW

**Message ID:** 13650

**Message Description:** LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_DEFAULT\_ALLOW

**Message Meaning:** Antiphishing reached default action without blocking the request.

**Type:** Web

**Category:** ANTIPHISHING

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
antiphishdc		string	64
antiphishrule		string	64
authserver	Authentication server for the user	string	64



Log Field Name	Description	Data Type	Length
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512

Log Field Name	Description	Data Type	Length
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13651 - LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_URL\_BLOCK

**Message ID:** 13651

**Message Description:** LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_URL\_BLOCK

**Message Meaning:** Antiphishing matched a URL filter rule and blocked the request.

**Type:** Web

**Category:** ANTIPHISHING

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
antiphishdc		string	64
antiphishrule		string	64
authserver	Authentication server for the user	string	64
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64

Log Field Name	Description	Data Type	Length
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13652 - LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_FTGD\_BLOCK

**Message ID:** 13652

**Message Description:** LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_FTGD\_BLOCK

**Message Meaning:** Antiphishing matched a Fortiguard category rule and blocked the request.

**Type:** Web

**Category:** ANTIPHISHING**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
antiphishdc		string	64
antiphishrule		string	64
authserver	Authentication server for the user	string	64
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6
msg	Log message	string	512

Log Field Name	Description	Data Type	Length
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3

## 13653 - LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_DEFAULT\_BLOCK

**Message ID:** 13653

**Message Description:** LOG\_ID\_WEB\_WF\_ANTIPHISH\_MATCH\_DEFAULT\_BLOCK

**Message Meaning:** Antiphishing reached default action and blocked the request.

**Type:** Web

**Category:** ANTIPHISHING

**Severity:** Warning

Log Field Name	Description	Data Type	Length
action	Security action performed by WF: blocked - url is blocked by webfilter passthrough - url is allowed by webfilter	string	11
antiphishdc		string	64
antiphishrule		string	64
authserver	Authentication server for the user	string	64
cat	Web category ID	uint8	3
catdesc	Web category description	string	64
craction	Client Reputation Action	uint32	10
crlevel	Client Reputation level	string	10
crscore	Client Reputation Score	uint32	10
date	Date	string	10
devid	Device ID	string	16
direction	Direction of the web traffic	string	8
dstintf	Destination Interface	string	32
dstintfrole	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
dstip	Destination IP	ip	39
dstport	Destination Port	uint16	5
eventtime	Web Filter event time	uint64	20
eventtype	Web Filter event type	string	32
fctuid	FortiClient UID	string	32
forwardedfor	X-Forwarded-For HTTP header	string	128
group	User group name	string	64
hostname	The host name of a URL	string	256
initiator	The initiator user for override	string	64
level	Log Level	string	11
logid	Log ID	string	10
method	Rating override method by URL domain name or IP address	string	6

Log Field Name	Description	Data Type	Length
msg	Log message	string	512
policyid	Policy ID	uint32	10
profile	Web Filter profile name	string	64
proto	Protocol number	uint8	3
rawdata	Extended logging data including HTTP method, URL, client content type, server content type, user agent, referer, x-forwarded-for	string	1024
rcvdbyte	Received Bytes	uint64	20
referralurl	Referrer URI	string	512
reqtype	Request type	string	8
sentbyte	Sent Bytes	uint64	20
service	Service name	string	36
sessionid	Session ID	uint32	10
srcdomain		string	255
srcintf	Source Interface	string	32
srcintfrole	Source Interface's assigned role (LAN, WAN, etc.)	string	10
srcip	Source IP	ip	39
srcport	Source Port	uint16	5
subtype	Log subtype	string	20
time	Time	string	8
trueclntip	True-Client-IP HTTP header	ip	39
type	Log type	string	16
tz	Time Zone	string	5
unauthuser	Unauthenticated user	string	66
unauthusersource	Unauthenticated user source	string	66
url	The URL address	string	512
user	User name	string	256
vd	Virtual domain name	string	32
vrf	Virtual router forwarding	uint8	3





**FORTINET®**



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.